

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.



1. Introduction

1.1 The Growing Need for Scam Resilience

Southeast Asia's digital economy continues to be a driving force of economic growth in the region. The digital economy's contribution to GDP in 2025 ranges from 8.40% to 23.90% across the Southeast Asia-6 countries.[1] With the signing of the ASEAN Digital Economy Framework Agreement (DEFA) this year, that contribution is expected to unlock up to USD 2 trillion in value, if the agreement is implemented well.[2]

This growth trajectory is projected to continue, driven by upward trends in digital finance and use of artificial intelligence (AI)-enabled services. As of 2025, digital channels in the region accounted for over 60% of transaction value.[3] This matters because payments are often the entry point to the wider digital economy, opening the door to credit, savings, and other financial services. In addition, AI is increasingly becoming part of daily digital use, through chatbots, translation, photo editing, and productivity tools. In 2025, around 79% of Southeast Asian workers reported having used AI, and over two-fifths have integrated these tools into both their personal and professional lives.[4]

However, this uptick in digital finance adoption and the growing sophistication of AI-enabled tools also presents its own risks, especially in the form of scams. As more people use digital financial services, for example, exposure to fraudulent activity also increases. The prevalence of AI tools and AI-enabled services has also made it easier to create convincing scam messages that target vulnerable users.

This compounds the growing cyber scam crisis in the region.[5] The United Nations reports that victims of transnational online scams across East and Southeast Asia, Australia and New Zealand have lost up to US$114.1 billion (S$147.2 billion) in 2025, with estimated losses at least tripling from 2023.[6] The combined prevalence and complexity of emerging schemes has the potential to affect user confidence and trust in the digital space. Loss of trust may lead to reduced digital participation, which, if exacerbated, may turn into wider-scale withdrawal from the digital economy. If left unchecked, digitally-enabled scams are thus a threat not just to individuals but to society as a whole.

There is a need to ensure that Southeast Asia develops resilience against scams. Scam resilience, as an extension of cyber resilience, is defined as the ability to anticipate, attack, withstand, recover from, and adapt once a scam attempt is made.[7] Various scam response models explored in TFGI's 2025 report, *Building Resilience Against Scams and Fraud in Southeast Asia: A Whole-of-Society Approach,* converge on resilience as the systematic integration of interventions throughout key stages: before, during, and after the scam.[8]

Previous reports have discussed the breadth and depth of systemic issues that hinder progress toward scam resilience in the region.[9] These include gaps around digital literacy, enforcement capacity, legal frameworks, and cross-border coordination that contribute to the complex scam landscape.

Apart from addressing systemic challenges, it is just as important to examine the degree to which individual confidence and scam detection skills act as building blocks for scam resilience. Confidence refers to a person's *self-perceived* ability to spot a scam. It shapes behaviour, which influences the likelihood of engaging in the digital economy. Skills refer to a person's *actual* capability to identify a scam and take the right action once one is detected. They determine a user's ability to navigate and mitigate online harms. The gap between the two is where the real vulnerability lies: when mindsets do not translate into meaningful action, or lead to disproportionate exposure to risks. The *confidence-skills gap* framework also offers an overall view of behaviours in the digital economy and potential levers to realise resilience.

The report aims to add to the conversation by reinforcing that scam resilience requires more than a policy and regulatory lens. It also requires a deep dive into lived experiences on the ground. Taking stock of Southeast Asians' scam encounters, confidence, scam detection skills, response plans, and the effects of scam attempts on digital participation provides evidence of whether the region's scam resilience efforts are realised by those they are intended to protect. Further, the report explores how the current scam landscape affects trust in digital systems, the extent to which lack of trust hinders meaningful digital participation, and the potential pathways for restoring lost trust. Lastly, it anchors on policy implications surfaced from the data to propose an initial set of recommendations and potential interventions throughout the scam lifecycle.

The next sections detail how the report unpacks these findings and provide context for interpreting the data through the methodology, scope and limitations, and an overview of key terms and concepts used.

1.2 Report Structure

To evaluate the progress of scam resilience efforts 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.

1.3 Terms and Concepts

The report adopts certain terminologies and concepts in its analysis, either previously conceptualised by the Institute or commonly used in the scam landscape. These are presented in the following paragraphs:

Scams are defined as a type of fraud relying on direct psychological manipulation.[10] Tactics create a sense of fear or urgency, leverage emotional appeal, and take advantage of limited knowledge and awareness to lead victims to authorise actions against their own interest. While the terms scams and fraud are often used interchangeably in Southeast Asia, no standalone legal definition of "scams" yet exists.[11] For this report, we will use the term "scams" throughout.

The following types of scams are widespread in the region and guide the design of the scam testing materials:

- **Phishing Scams.** These are fraudulent attempts to obtain sensitive information (such as login credentials, banking details, or Transaction Authorisation Codes) by masquerading as trustworthy entities. These schemes typically appear through email, text messages, or instant messaging platforms such as WhatsApp, exploiting the ubiquity of digital communication.[12]
- **Fake Lottery/Sweepstakes/Prize Scams.** These scams, also known as unexpected money scams, work by notifying users that they have won a lottery or competition they did not enter, and asking them to pay a fee in order to claim winnings.[13] Variations include asking for payment to increase odds of winning and requesting personal or financial information as a requirement for claiming.[14]
- **Impersonation of Authority Scams.** Impersonation scams involve fraudsters posing as trusted authority figures, such as government officials, police officers, or corporate representatives, to manipulate victims into complying with fraudulent requests.[15] Common narratives include claims of unpaid fines, involvement in criminal investigations, or urgent administrative issues requiring immediate attention.
- **Love/Romance Scams.** Romance scams target individuals seeking emotional or romantic connections, and often begin on online platforms, such as dating applications and social media networks, where scammers can easily create elaborate false identities.[16] The relationships develop gradually, with scammers investing weeks or months to build emotional intimacy through consistent communication, flattery, and fabricated life stories. Once sufficient trust is established, the scammer introduces a sudden crisis, such as medical emergencies, travel difficulties, or legal problems, and requests immediate financial assistance.

- **Job/Task/Employment Scams.** These schemes involve false promises of lucrative employment opportunities, often requiring upfront payments for processing fees, training costs, or travel documentation.[17] Victims may be required to provide extensive personal information or pay substantial fees for purported "visa processing" or "job placement" services, only to discover that the employment opportunity is non-existent or part of a larger exploitative scheme involving forced labour or cryptocurrency fraud.
- **E-Commerce Scams.** These scams involve the sale of goods and services through e-commerce platforms or social networking sites, without physical meet-ups prior to the confirmation of sale. Scammers put up fraudulent listings that typically require payment upfront and may never deliver the goods or services, send a product that does not match the listing, farm personal and financial information through third-party links, or even charge additional fees after confirmation of sale.[18]
- **Deepfake Scams.** Deepfake scams represent one of the most technologically advanced forms of fraud, utilising Artificial Intelligence (AI) to create highly realistic yet entirely fabricated audio or video content. These schemes typically involve impersonating public figures or trusted individuals to promote fraudulent investment opportunities, products, or services.[19]

Other concepts that will be periodically referred to throughout the document:

- **Scam literacy.** While no official definitions exist, its meaning can be derived from existing constructs and measurements pertaining to literacy. Literacy is defined as the knowledge and set of skills that enable individuals to understand information and make effective decisions.[20] Integrating this with the definition of scams, scam literacy can thus be understood as the knowledge and set of skills enabling individuals to recognise and avoid fraudulent schemes that leverage deception and psychological manipulation.
- **Scam resilience.** This is conceptualised in TFGI's 2025 report as the systematic integration of well-timed, coordinated actions throughout the entire scam lifecycle (before, during, and after the scam, and long term).[21] It postulates that resilience is composed of four intervention pillars: Protect, Identify and Detect, Respond and Recover, and Adapt.[22] It thus spans prevention, mitigation and recovery measures against scams.

These terminologies are explored further in the following reports: *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of-Society Approach*[23] and *Towards a Resilient Cyberspace in Southeast Asia.*[24]

1.4 Methodology

The report primarily uses data collected through a quantitative survey. Respondents were recruited via online panels in Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam. In July 2026, a sample of 1,000 respondents aged 18 to 70 was collected in each country, for a total of 6,000 respondents. For each country, the collected samples were controlled with quotas mirroring the national demographic distributions for age, gender and ethnicity. Sampling assumes a confidence level of 95%,[25] with an indicative margin of error (MOE) of 1%.[26] Country samples are unweighted when aggregating data to generate regional performance; that is, each respondent is treated as equally important regardless of which country they were drawn from.

Recruitment involved randomised sampling, respondent screening, and a pre-testing phase before full survey rollout. Respondents were randomly selected from a range of online panels to take the survey. A basic screener was used to filter out those with potential conflicting interests, such as market research employees. Fieldwork preparations included initial quality checks ensuring the questionnaire was correctly programmed, followed by a soft launch to 30 respondents per country to assess any issues with data collection. Once pre-testing was cleared, the survey was launched widely, with continuous quality checks done back-end on the integrity and quality of responses.

The survey and accompanying scam testing materials were designed in English and later translated to local languages. Respondents were given the option to take the survey in either English or their local language.

The questionnaire was structured in the following order: exposure, confidence, identification skill, response plan, and trust and recovery. This flow was determined to ensure that stated confidence levels would not be affected by the outcome of the identification skill module. Priming concerns regarding the scam identification module were mitigated by past data from similar testing flows where respondents did not necessarily perform better,and may even perform worse, despite knowing the survey was scam-related upfront. Responses and scam testing materials were randomised to discourage response automation, with back-end quality checks done to discard responses according to parameters such as speed of answering.

Confidence in detecting a scam attempt was rated on a 6-point scale, where 1 meant "Not confident at all" and 6 meant "Highly confident". Respondents were considered confident in detecting scam attempts based on selecting the top 2 box (T2B) responses: 5 ("Confident") and 6 ("Highly confident").

To measure skill in identifying scams, seven sets of imagery or audio were created. Respondents were shown the following types of scams: phishing, job/task, e-commerce, government/authority, love, and AI impersonation/deepfake scams. These scam types were previously identified as among the most concerning in the region.[27] A legitimate government-sent message was also shown as a control. With the exception of the legitimate message, the scam imagery or audio were the same for all countries, with translated versions provided for those who opted to take the survey in the local language. The legitimate message varied based on the language, the government agency/authority which sent the message, and the message content.

While derived from genuine scam references, details found in the scam imagery are fictitious and are created with the support of generative Artificial Intelligence (Gen AI) tools. The image below provides a sampling of the scam materials used.



After viewing the stimulus, respondents were then asked to determine whether or not it was a scam on a 6-point scale, where 1 meant “Definitely not a scam” and 6 meant “Definitely a scam". This was later followed by a question on what they would do first upon encountering that type of scam, including options deemed risky behaviour.

The scoring of actual skills comprises correct identification and selection of a safe action in response to each hypothetical encounter. Per stimulus, respondents can earn 0 to 2 points: +1 for correctly identifying an attempt and +1 for selecting a safe action. The highest attainable score is 14 points (2 points per scam type, multiplied by 7 types). The skill score is then normalised to fall within 0-100, where 100 is the highest, through the following calculation: (Raw score / Highest attainable score) x 100.

Scam response readiness is a separate metric that evaluates the safety of respondents’ actions during and after a scam attempt, and their awareness of where to report an attempt. High response readiness is achieved if the respondent chooses only safe actions during and after an attempt, and is clear about where to report an encounter. Performing safe actions either during or after a scam, and some hesitance regarding where to report, is seen as moderate response readiness. Response readiness is considered low if a risky action or no action at all is taken, at either stage of an attempt, or if the respondent does not know where to report a scam.

1.5 Scope and Limitations

The report focuses on the overall state of scam resilience in Southeast Asia-6 (Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam). It adopts a regional framing of the results throughout. Recommendations are similarly provided through a regional lens. Further investigation is thus necessary to understand areas such as why certain behavioural patterns occur and how effective current interventions are on the ground. Stakeholder consultations are also needed to generate a more comprehensive and detailed set of recommendations. Nevertheless, the recommendations offer a general direction of travel for potential policy actions to develop a resilient digital society against scams.

The interpretation of survey findings is subject to the following limitations:

- To ensure completion, and due to the method of dissemination (i.e., online), the survey is designed to be completed in a single sitting. It is unable to replicate the time and effort expended by scammers today to gain their victims' trust. Due to this, respondents can only be tested on their ability to identify scam imagery based on the singular moment of being presented with the stimulus.
- To minimise the automation or routine selection of responses, quality checking is done post-survey completion, and responses are removed if they do not meet specific parameters such as answering speed.
- The survey recognises that there may be underlying bias in reporting scam encounters or victimisation; efforts have been made to minimise this through an upfront disclaimer of anonymisation of data and the framing of questions in objective language.
- Priming may also be a concern. Understanding that the survey's subject matter is scams may have induced a heightened vigilance among respondents when taking the skill identification module. However, this also means that lower-scoring performances may be more worrying in reality. Past data of similar testing flows have shown that respondents do not necessarily perform better, or may even perform worse, despite knowing the survey is scam-related upfront. The results of this survey's scam identification module are also varied rather than generating a universally high performance across stimuli, which may have been observed if priming were in effect.



2. The State of Scam Resilience in Southeast Asia

Southeast Asia's progress toward scam resilience is defined by how empowered users feel throughout the scam lifecycle. Before, during and after the scam, there are opportunities to prevent, mitigate and recover that can be further enhanced in the long term. Anchoring on TFGI's Cyber Resilience Framework,[28] a structured approach can be developed for targeted interventions at each stage. It is comprised of four pillars:

- **Protect.** The Protect phase centres on reducing the incidence and potential damage of scams through proactive, preventive measures. These can involve digital literacy and behaviour change campaigns.
- **Identify and Detect.** In this phase, the focus is on detecting, verifying, and intercepting scam threats in real-time before financial or emotional damage occurs. Institutional and citizen-driven reporting play a role at this point in an incident.
- **Respond and Recover.** The Respond and Recover phase is the enhancement of individual and societal capacity to act swiftly and effectively after a scam has occurred. During this phase, scams can be disrupted while victims are supported through empathy-led assistance
- **Adapt.** This phase prioritises strengthening the long-term capacity of societies to stay ahead of emerging and evolving scam threats. Typically, this is when regulations are enhanced, the responsiveness of legal systems is improved, and national anti-scam strategies are stress-tested to address potential exploits.

The figure below illustrates the scam lifecycle and the proposed intervention pillars:

Figure 1. Targeted Interventions throughout the Scam Victim Journey



Source: Tech for Good Institute, 2025

This chapter discusses insights from the survey on the scam victim journey in Southeast Asia, viewed through the lens of whether incidents and interventions through the years have affected behaviours. Chapter 2.1 explores the factors that drive scam exposure and victimisation in the region, and whether measures to *Protect* need to be re-contextualised. Chapter 2.2 contrasts self-reported confidence versus observed ability to correctly *Identify and Detect* attempts, and assesses the vulnerabilities that emerge when there is a gap between self-perceived and actual skill. Whether users know how to safely *Respond* to scams and how they can *Recover* from the experience is evaluated in Chapter 2.3, as a measure of how aware users are of the high-level policies and mechanisms in place to mitigate scam losses. Lastly, Chapter 2.4 looks into the impact of scam encounters on digital participation and identifies the levers for how users and societies can *Adapt* to the ever-changing scam landscape.

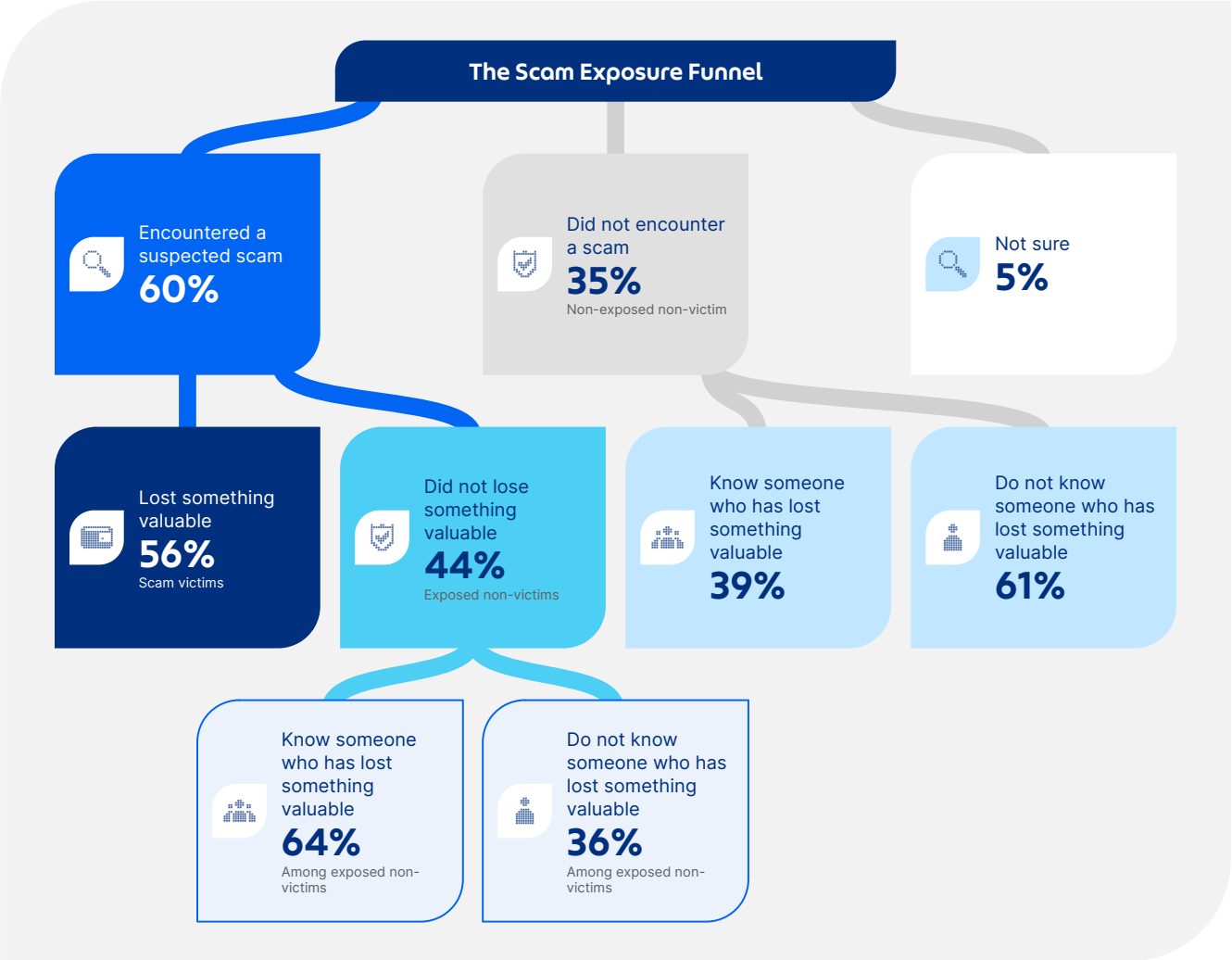
2.1 Protect: The Exposure Risk

Scam exposure across Southeast Asia is widespread, driven by digital activity rather than consistent demographic patterns. The risk is no longer specific to conventionally vulnerable population segments like the elderly. The youth (18-34 years old) and the workforce, for example, are seeing higher frequencies of scam encounters and consequent losses. Apart from this, analysing exposure and victimisation by other demographic factors such as gender does not yield significantly different results. This indicates that scam risks are more broadly distributed than originally believed. The depth of digital participation also plays a role in determining vulnerability – not just the frequency of internet usage, but the types of online platforms they engage with.

Scams have expanded beyond known typologies. Survey results show that the top scams encountered in the region are prize scams, job scams, and phishing scams. Of these three types, only phishing scams (35%) are considered by respondents to be concerning, alongside new schemes like impersonation of authorities (31%) and fake bank, e-wallet or payment notifications (29%). AI scams are joining the mix, with 19% encountering an AI-generated impersonation and 14% through an AI chatbot, digital assistant or automated agent. This leads to growing worry and concern about the difficulty of detecting the various types of scams (64%).

More than half of scam encounters in Southeast Asia result in the loss of money, personal information, accounts or other valuables. Out of the three in five respondents who have encountered a scam attempt in the past year, 56% reported falling victim. Even among the 44% who were exposed but avoided loss, 64% know someone who has lost something to a scam. The likelihood of an attempt leading to a loss is thus high. Additionally, 39% of those who have not encountered a scam still know at least one scam victim. This shows that scams are prevalent enough in the region that awareness of victimisation is high regardless of personal exposure.

Figure 2. The Scam Exposure Funnel

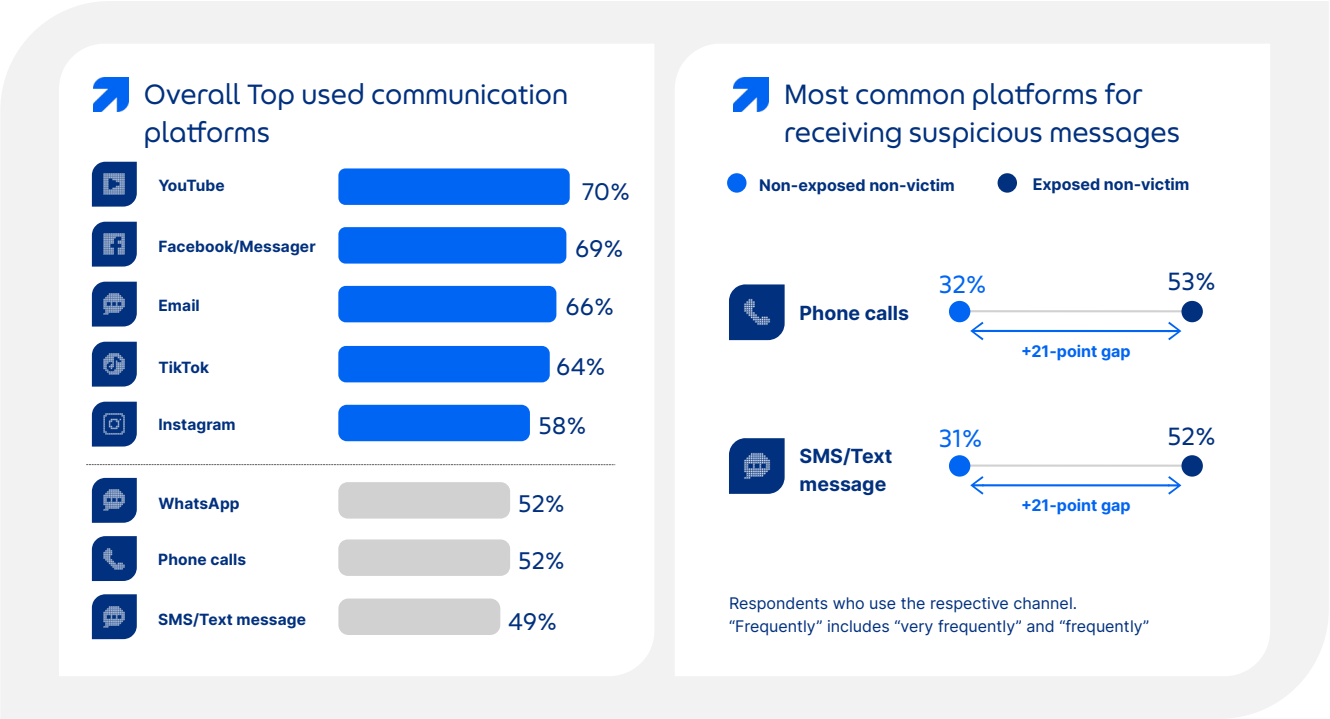


Includes data from the following questions: C1. In the past 12 months, have you personally encountered any suspected scam or fraud attempt?; C2. In the past 12 months, have you personally lost money, account access, personal information, or anything valuable because of a scam or fraud incident?; C3. Do you personally know someone who has lost money, account access, personal information, or anything valuable because of a scam or fraud incident in the past 12 months? Scam victims are those who have lost something valuable to a scam. Exposed non-victims have encountered an attempt but have not lost anything of value. Non-exposed non-victims have not encountered a scam and have thus not lost anything valuable.

Source: Tech for Good Institute, 2026

What drives scam exposure, however, is the depth of digital participation more than any other factor. Those who have encountered a scam show higher levels of engagement across a variety of platforms, notably work platforms and AI tools, than those who have not. More interestingly, they report significantly higher instances of receiving suspicious communications regardless of platform, but especially through SMS and phone calls. This suggests that their personal or account information may have already been compromised prior to the encounter, potentially due to the extent of their digital participation.

Figure 3. Depth of Digital Participation as a Driver of Scam Exposure

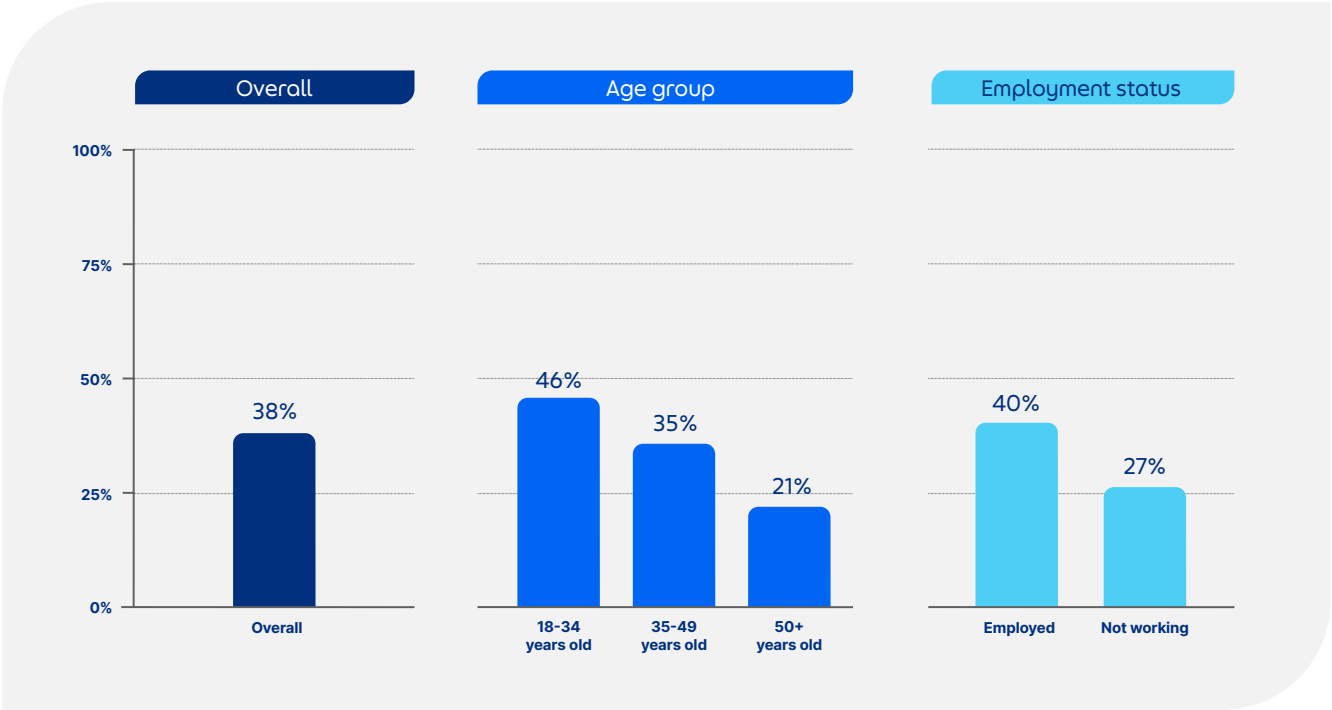


Includes data from the following questions: D1. Which of the following communication channels or platforms did you use in the past 12 months?; D3. From the channels you selected, how often do you receive suspicious messages, calls, posts, listings, or requests on each channel?

Source: Tech for Good Institute, 2026

Within today's highly connected environment, younger and economically active respondents are more exposed than other groups. 65% of those aged 18–34 and 62% of those employed have encountered a suspected scam. They are also more likely to report having lost something of value to scammers, at 46% and 40%, respectively. Older age groups and those who are unemployed report lower rates of loss, challenging the stereotype that scam victims are predominantly older or conventionally vulnerable people.

Figure 4. Scam Victimisation by Age Group and Working Status



Includes data from the following questions: C2. In the past 12 months, have you personally lost money, account access, personal information, or anything valuable because of a scam or fraud incident? Overall refers to all respondents who have taken the survey. Not working is composed of students and unemployed individuals.

Source: Tech for Good Institute, 2026

But vulnerability to scams still appears broadly distributed rather than concentrated in identifiable groups. Scam exposure and victimisation rates are similar across other demographic factors, including gender, educational attainment and financial capability. And while older age groups now appear less likely to be victims than the youth, they are no less at risk.

Preventative measures need to reflect the universality of scam exposure. Scam encounters occur across channels, countries and demographic groups. It remains important to cater to traditionally at-risk segments, such as those in rural areas or the isolated elderly, but scam campaigns should be designed for the wider population as well. Ensuring the quality of user knowledge in navigating scam attempts is just as important, as the following sub-chapters explore Southeast Asians' skills in detecting and responding to scams.

2.2 Identify and Detect: The Confidence Trap

A persistent gap exists between people's confidence in detecting scams relative to their demonstrated skills, which may affect how they respond to attempts down the line**.** The disconnect plays out differently and can be classified into four personas that characterise Southeast Asians' differing approaches to scam detection. While overall scam recognition appears strong, it can obscure weaknesses in identifying certain types of scams, such as impersonations. Crucially, neither experience nor confidence is a reliable predictor of actual skill. Previous scam victims, for example, do not perform better than non-victims. Similarly, there are those with high confidence but are not accurate in identifying attempts.

Southeast Asians are underconfident despite relatively strong scam recognition. Only around two in five profess confidence in their ability to detect a scam. But when asked whether seven different stimuli were scams, respondents correctly assessed them seven out of ten times on average (71%). A strong overall score, however, does not translate into consistent ability across the wide range of threats. Recognition is strongest for AI family emergency or impersonation scams (85%) but falls to 60% for government or police impersonation scams.

The figure below illustrates the gap, in percentage points, between confidence and skills for the different groups: overall, or all respondents of the survey; by age group; by whether or not they have encountered a scam; and by whether they have been a scam victim.

Figure 5. The Confidence-Skills Gap



Scores shows the percentage points gap between confidence and actual skills, combining scam identification, safe action and reporting clarity. Positive values indicate confidence exceeds skills; negative values indicate the reverse. Includes data from the following questions: C5. How confident are you in your ability to detect scams or fraud attempts?; F1_1 to F1_7. Do you think this is likely to be a scam, fraud attempt, or fake content?; G1. If you suspect that you are being targeted by a scam, but have not lost money or information yet, what would you most likely do?; G2. If you became a victim of a scam or fraud and lost money, account access, or personal information, what steps would you take?; G3. How clear are you about where to report a scam or fraud incident in your country?

Source: Tech for Good Institute, 2026

Four personas emerge when mapping consumers based on their confidence level and skill at identification. Scoring High on each dimension requires at least a 60 on a 100-point scale; a score below 60 is classified as Low. Personas are considered to have High confidence when they respond at least a 4, or “somewhat confident", on a 6- point scale, resulting in a score above 60 on the horizontal axis. Meanwhile, the score for actual skills aggregates points from correctly identifying and safely responding to each scenario, earning up to 14 points. To be considered as having High actual skills, respondents need to have a raw skill score of at least 8 to achieve 60 when converted to a 100-point scale. **Chapter 1.4** details the scoring logic for each dimension further.

The figure below provides a conceptual mapping and description of the four personas based on these two dimensions:

Figure 6. Scam Detection Personas in Southeast Asia

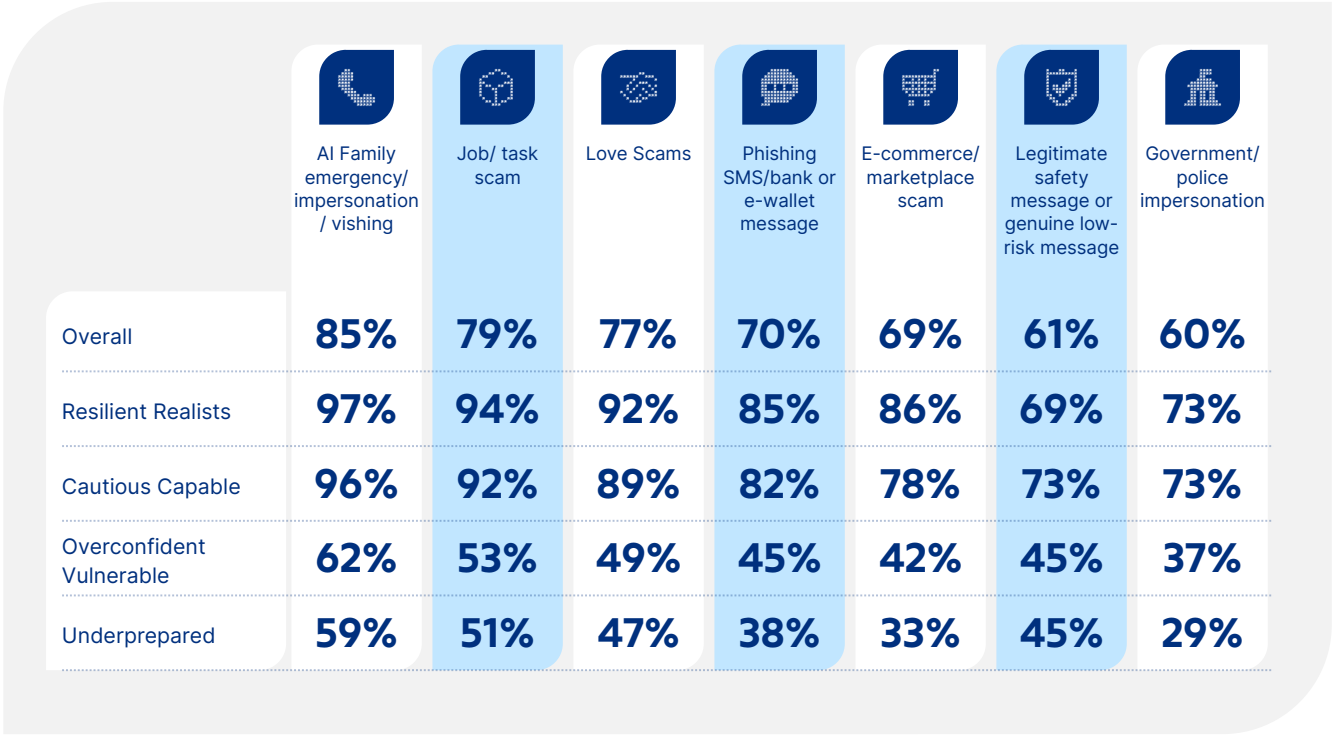


Source: Tech for Good Institute, 2026

Based on this framework, the majority of respondents are Resilient Realists (55%), followed by the Overconfident Vulnerable (29%). The rest are split into the Cautious Capable (10%) and the Underprepared (6%). **Box 1** at the end of the sub-chapter describes the personas in depth.

The scorecard below illustrates the variance in how the different personas perform across the seven scam detection tests. Resilient Realists can correctly detect a scam attempt more than 80% of the time, for five out of the seven scenarios. In comparison, less than half of the Undeprepared are likely to correctly identify an attempt for the majority of the tests, with performance dropping as low as 29% for government or police impersonation scams.

Figure 7. Seven-Test Scorecard



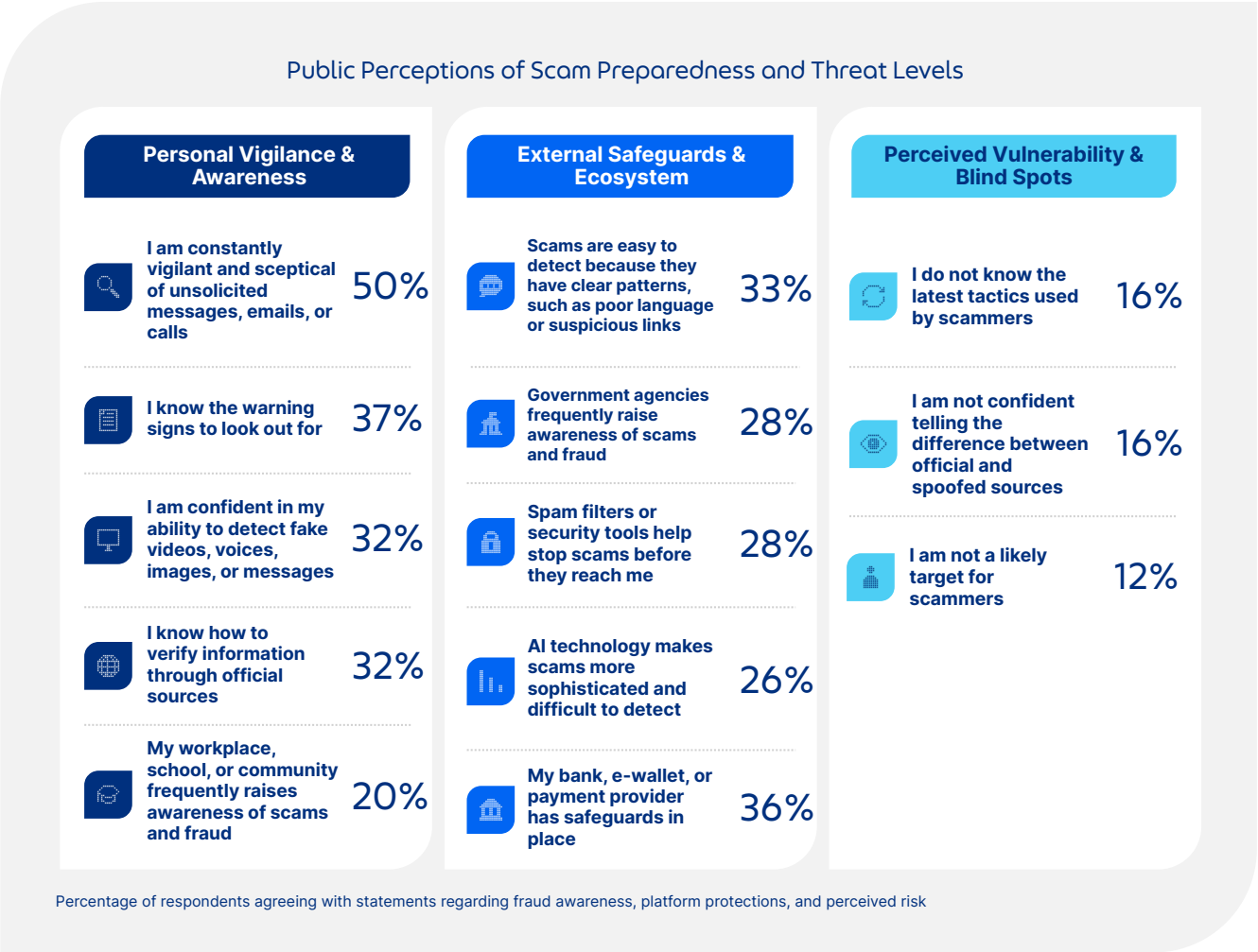
Includes data from the following questions: F1_1 to F1_7. Do you think this is likely to be a scam, fraud attempt, or fake content?

Source: Tech for Good Institute, 2026

Experience does not necessarily lead to better skills. Whether or not a user has been exposed to scams, there is no significant difference in their identification scores (those who have encountered a scam: 73%, those who have not encountered a scam: 70%). More worryingly, scam victims are slightly predisposed to take risky actions even if they suspect the transaction is a scam attempt (58% vs. 43–44% for non-victims).

Another concern is Southeast Asians' confidence being anchored in suspicion rather than established knowledge. Personal vigilance is the primary driver for how users assess an attempt (50%). Awareness of online safeguards ranks lower, such as knowing the warning signs of a scam (37%). This may be a potential exploit as the appearance of legitimacy attracts considerably less scrutiny. Examples include the use of personal details in communications or websites that look professional. These cues may not be inherently suspicious, but neither do they provide proof of authenticity.

Figure 8. Public Perceptions of Scam Preparedness and Threat Levels



Includes data from the following question: C6. What makes you feel confident/not confident in your ability to detect scams or fraud?

Source: Tech for Good Institute, 2026

This also points to a growing inclination toward hypervigilance. For example, 61% correctly recognised the legitimate message as not a scam, while the rest viewed it suspiciously despite lacking typical markers such as hyperlinks. While 61% is high, it is among the scenarios where respondents were the least accurate in their assessment. This is concerning, because scepticism may help consumers guard against scams, but it may also have undesired effects on digital participation. Fewer genuine transactions may be completed, for example, or important communications ignored due to paranoia. It is important that users maintain a healthy amount of guardedness, enabling them to continuously navigate online spaces without fear.

The ideal outcome is that confidence is backed by the necessary skills in scam detection. Sizeable gaps between the two can breed vulnerabilities. Underconfidence despite having high demonstrated skills may induce hesitation and avoidance, while overconfidence despite weaker skills may lead to unfounded risk-taking. Striking this balance is a moving target, but having a clear view of user profiles across Southeast Asia offers an opportunity to focus on potential policy mechanisms to help shape how users engage the digital ecosystem.

Box 1. Characterising the Scam Detection Personas in Southeast Asia	
Resilient Realists	**Resilient Realists** are confident in their skills and are capable of identifying scams. They are also capable of responding safely after a scam has occurred. Despite experiencing the same level of scam exposure as the overall population (60%), they are less likely to end up losing anything valuable (31%). Their primary response to any type of scam is to block or delete the attempt, followed by reporting it, demonstrating a high awareness of safe actions.
Cautious Capable	**Cautious Capable** have a tendency to underestimate their skills, but they perform well in scam scenarios. Similar to Resilient Realists, scam encounters (56%) are less likely to end up in a loss (33%) compared to other personas. Part of this may be due to significantly higher levels of scepticism in the safety of digital services. Their immediate response, across scam types, is to disengage by blocking or deleting, followed by reporting and verifying the attempt with authorities.
Overconfident Vulnerable	**Overconfident Vulnerable**, on the other hand, overestimate their skills. Their performance in identifying and responding to scams is weak. They are slightly more exposed to scams than average (63%) and are substantially more likely to have lost something of value (52%). Their overconfidence may make them more likely to engage in risky behaviour, such as continuing to engage with the scammer and sharing suspicious links to warn others.
Underprepared	**Underprepared** respondents have low confidence and weak demonstrated skills. Although they have the lowest reported scam exposure of the four personas (50%), they are the second most likely to have lost something of value (45%). Less exposure to information about scams, potentially due to lower digital participation, leads them to be unsure of what to do in response to different scam types. They are also more likely to click on suspicious links and contact the scammer.

2.3 Respond & Recover: The Action Gap

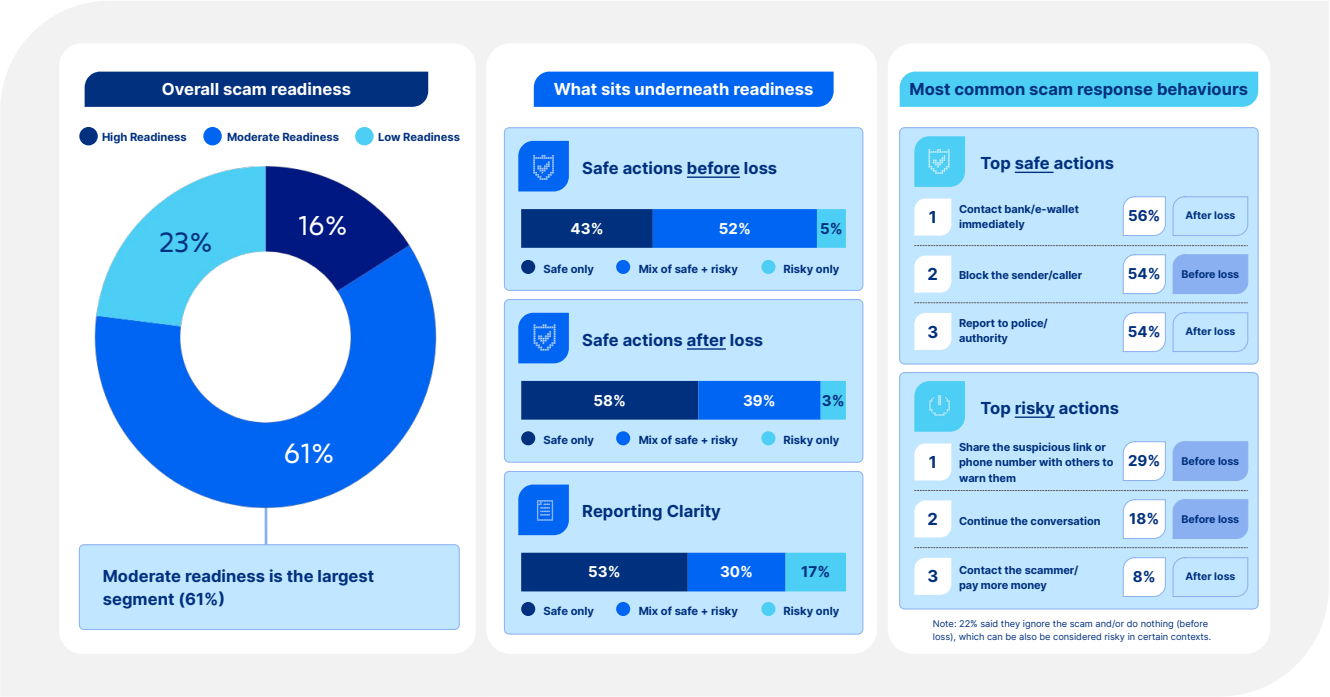
The region's ability to respond and recover once a scam attempt succeeds remains limited. Most Southeast Asians demonstrate uncertainty in reporting and at times take risky actions that can deepen the harm. Being unable to grasp which actions are safe or not may contribute to victims continuing to fall for subsequent attempts. Encounters also leave lingering effects. Many of the respondents have made changes to their digital behaviours due to concerns about scams. Longer term, there are efforts being made to improve victim support and recovery. However, the data reveals a subconscious inclination to assign blame despite publicly advocating for empathy.

In the immediate period after a scam has occurred, the priority shifts toward reducing the impact of the harm. Users can support this by individually developing scam response readiness. This is defined as having a scam response plan that is clear about who to engage, how and when, in order to mitigate the negative effects of a scam encounter. In the context of this report, scam response readiness is measured based on whether a user selects safe actions when asked about their response to a suspected scam attempt. An action is deemed unsafe if it has the potential to increase damage, such as by continuing to engage with the scammer. Scam response readiness also accounts for whether users know where to report incidents, as this contributes to broader anti-scam measures. For further details on the scoring logic, refer to **Chapter 1.4**.

Southeast Asia is only moderately scam-ready. At least 61% of respondents take a risky action when they suspect they have encountered a scam, or after they have fallen victim to one. The most common response to an attempt is to block the sender or caller, which is not inherently unsafe. But if the attempt is not reported, there is a missed opportunity to contribute to broader investigation and takedown efforts. The tendency to share a suspicious link publicly to warn others (29%) is another concern. While done with good intentions, exposing users to a link, even with context provided, can still lead to them accidentally clicking on the link and being victimised. To understand which actions are considered safe, risky or neutral, refer to **Box 2** at the end of this section.

Worryingly, only 53% are clear about where to report a scam in their country. Fragmented response systems may contribute to this.[29] The gaps in individual scam response readiness may simply be mirroring gaps in societal measures. When there is a lack of clarity regarding scam response procedures, victims may not seek institutional response mechanisms and may not be able to report the incident even if they want to. They may also choose to take things into their own hands to recover their lost funds.

Figure 9. Scam Readiness in Southeast Asia



Scam readiness is derived through correct scam identification, safe actions, and reporting clarity. Includes data from the following questions: G1. If you suspect that you are being targeted by a scam, but have not lost money or information yet, what would you most likely do?; G2. If you became a victim of a scam or fraud and lost money, account access, or personal information, what steps would you take?; G3. How clear are you about where to report a scam or fraud incident in your country?

Source: Tech for Good Institute, 2026

But the more pressing issue is the tendency for repeated victimisation. Data shows that scam victims perform slightly worse than non-victims in identifying scam attempts (67% vs 74%). They are also significantly more likely to engage in risky actions, like paying scammers money to return their fund, than exposed non-victims. Of concern is that they are more likely to freeze up in response to an encounter, doing nothing because they're embarrassed or simply don't know what to do. Inaction as the immediate response is in itself not risky, but that moment of uncertainty can be a window for scammers to sway their target. Though only a small proportion of victims act this way, it is worth noting that scammers do not need to convince every person they contact. Extracting high value from a select few is enough to make their payday.

Scam encounters clearly leave a mark. While only 38% of scam victims say they have been personally affected by the experience, the majority have changed their digital behaviour in some way due to concerns about scams. This concern extends further. Only 16% of non-victims report no changes to their digital behaviour, whether or not they have had previous exposure. Apart from increasing protective measures, users are beginning to retreat from digital spaces: avoiding new digital services or apps (23%) and using cash more often instead of digital payments (21%).

Figure 10. Behavioural Actions Taken

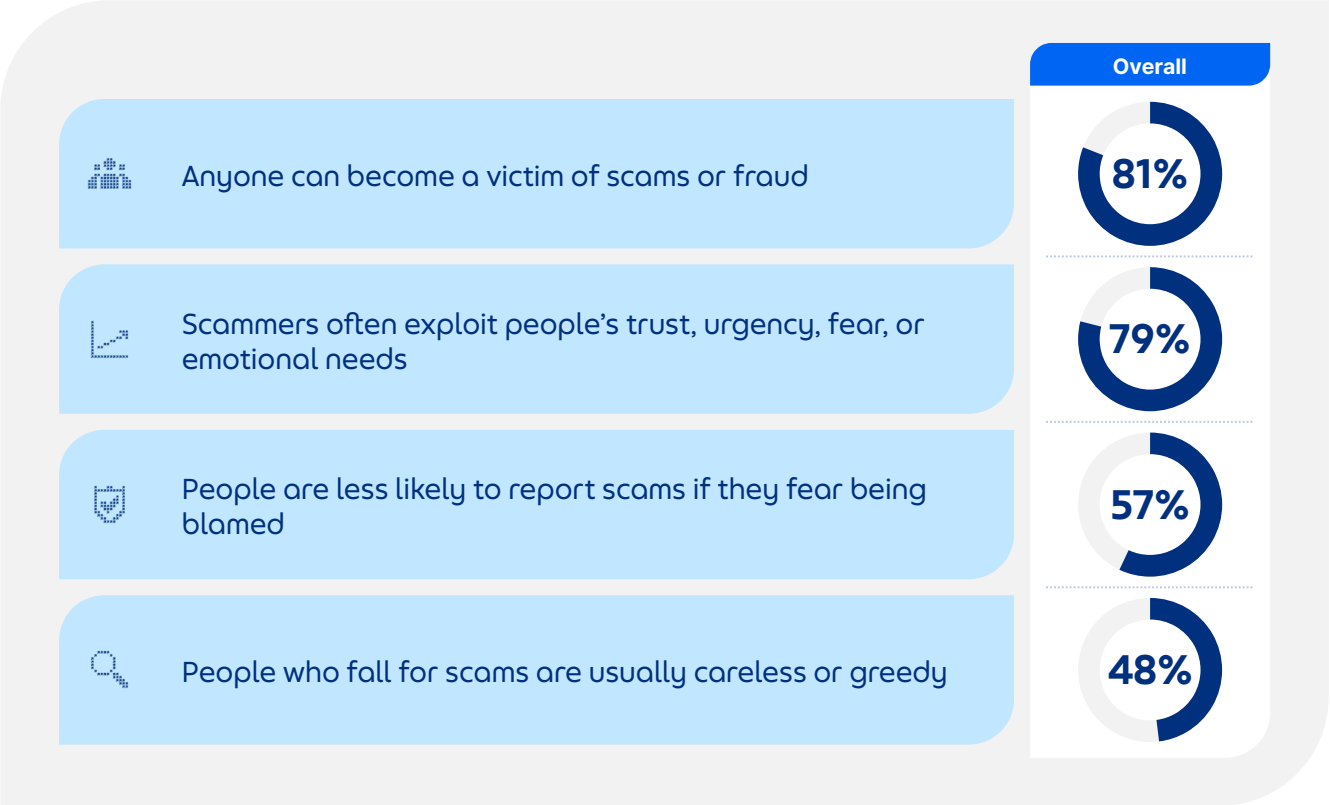
Responses	Overall	Victim of a scam	
Avoidant behaviour		**Yes**	**No**
Avoided clicking links even from known organisations	**46%**	**46%**	**45%**
Avoided trying new digital services or apps	**23%**	**28%**	**20%**
Avoided making online purchases	**14%**	**20%**	**11%**
Digital Economy Withdrawing Behaviour		**Yes**	**No**
Used cash more often instead of digital payments	**21%**	**28%**	**17%**
Reduced my use of online banking or e-wallets	**18%**	**24%**	**14%**
Stopped using or reduced use of social media or messaging apps	**17%**	**24%**	**13%**
Scam protection behaviour		Yes	No
Spent more time verifying information before acting	**46%**	**46%**	**36%**
Installed or updated security tools	**32%**	**36%**	**30%**
no change in behaviour		Yes	No
No, my digital behaviour has not changed	**12%**	**4%**	**16%**

Includes data from the following question: I2. Have concerns about scams or fraud caused you to do any of the following in the past 12 months?

Source: Tech for Good Institute, 2026

In addition, public attitudes toward scam victims reveal a tension between empathy and blame. Majority (78%) believe victims should be able to report scams without embarrassment and recognise that anyone can become a victim (81%). There is also broad recognition of how scams work, with 79% agreeing that scammers exploit trust, urgency, fear or emotional needs. Despite this, 48% of respondents believe that people who fall for scams are usually careless or greedy. Scam victims are also more likely to attribute victimisation to a failure of personal judgement, which can later increase reluctance to report incidents due to fear of being blamed.

Figure 11. Perceptions of Scam Victimisation



Includes data from the following question: I5. To what extent do you agree or disagree with the following statements about scam victims?

Source: Tech for Good Institute, 2026

Scam readiness programmes are best positioned to bridge knowledge and action gaps. They can provide a focal point for understanding the difficulties or barriers users may have in leveraging the protections available to them, and coordinating with relevant authorities, institutions and platforms to address these concerns. The ideal result is an effective and adaptive scam response plan that users can easily draw on during and after an encounter.

Moreover, victim care and support is a necessary component of scam response. Shame can become another barrier to recovery. If victims expect to be judged, seeking help may become more difficult, even in environments that appear outwardly supportive. Reducing victim blaming hinges on creating the conditions that make people feel safe and heard. This is not limited to reframing the language around scam awareness campaigns. It includes the provision of ethical and professional care, such as mental health support, and access to legal and financial assistance.

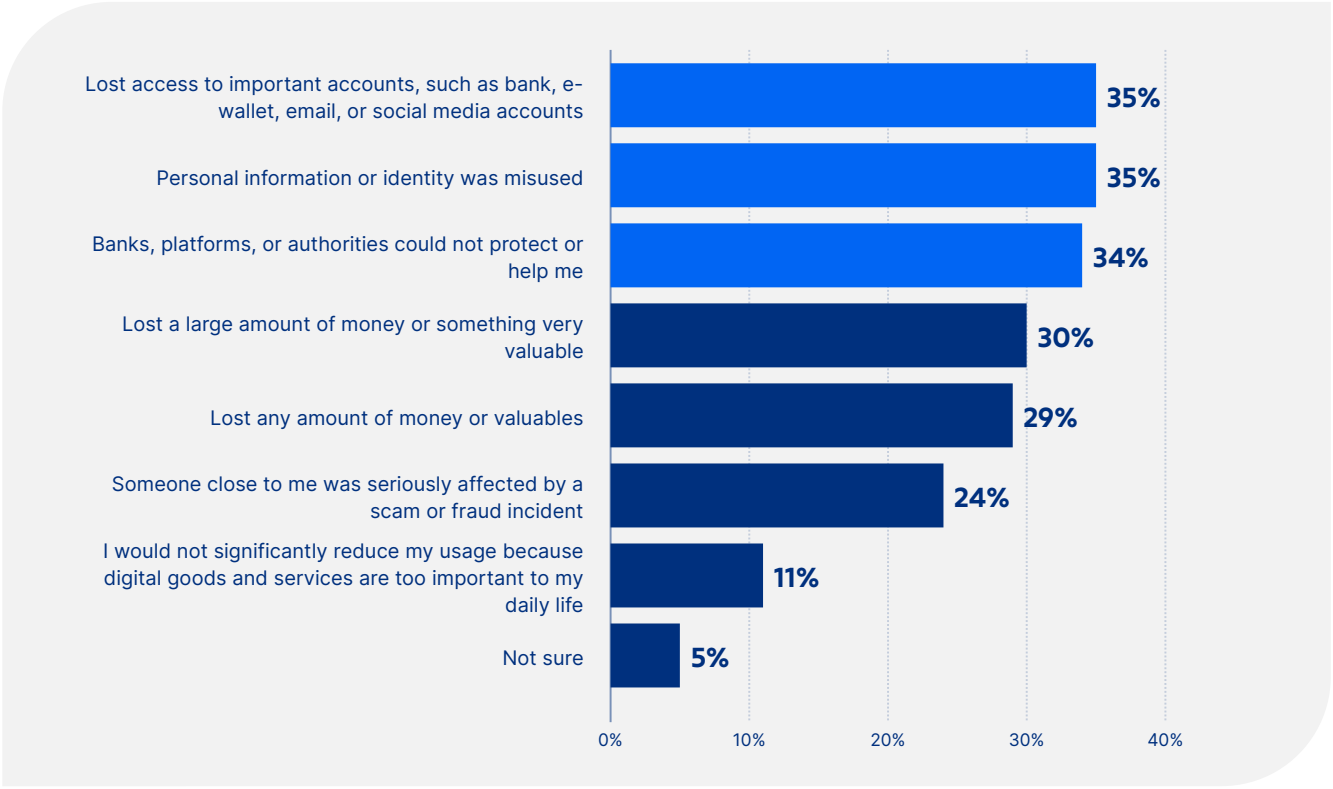
Box 2. Differentiating between Safe, Risky and Neutral Actions in Response to Scams	
Safe Actions	Actions that are protective and aim to reduce, mitigate, or altogether prevent the negative impact of a scam. They may involve leveraging existing online safeguards. Examples include reporting an attempt on official channels, contacting the related platform to block or reverse the transaction, and checking whether other accounts may be affected.
Risky Actions	Actions that may unintentionally open a user up to further exploitation by the scammer. They may involve continued engagement with the scammer. Examples include directly negotiating with the scammer to return the funds, continuing the conversation to get more proof, and sharing the link publicly to raise awareness. The latter is considered risky, as others may go straight to clicking the link without paying attention to why it is being shared, potentially leading to more victims.
Neutral Actions	Actions that can neither be categorised as protective or directly harmful. This includes doing nothing and not knowing what to do. While they do not necessarily lead to further harm, they can be concerning, especially if they lead to a moment of uncertainty that scammers can exploit.

2.4 Adapt: The Trust Build

Longer term, sustaining trust in digital systems is a key objective for scam resilience efforts. Scams do not only change digital behaviours; data from the survey shows that they can weaken trust in platforms and reduce digital participation. Users lean on institutional response mechanisms, such as stronger safeguards, to recover trust when it is lost. But feelings on whether institutions deliver on this expectation are mixed. There are those who feel they are left to handle scam risks alone. And others, though few, say their trust cannot be restored once it is lost.

Building back trust once it is undermined by an encounter is central to sustaining digital participation. For example, only 11% of respondents noted that they would not significantly limit participation in the digital economy due to scams. This implies that for the vast majority, withdrawal from the digital economy is an ever-present possibility if scams are left unchecked. For many, losing access to accounts, their personal information being misused, or the perceived lack of institutional support turns that possibility into a certainty.

Figure 12. Impetus to Reduce Interaction with the Digital Economy

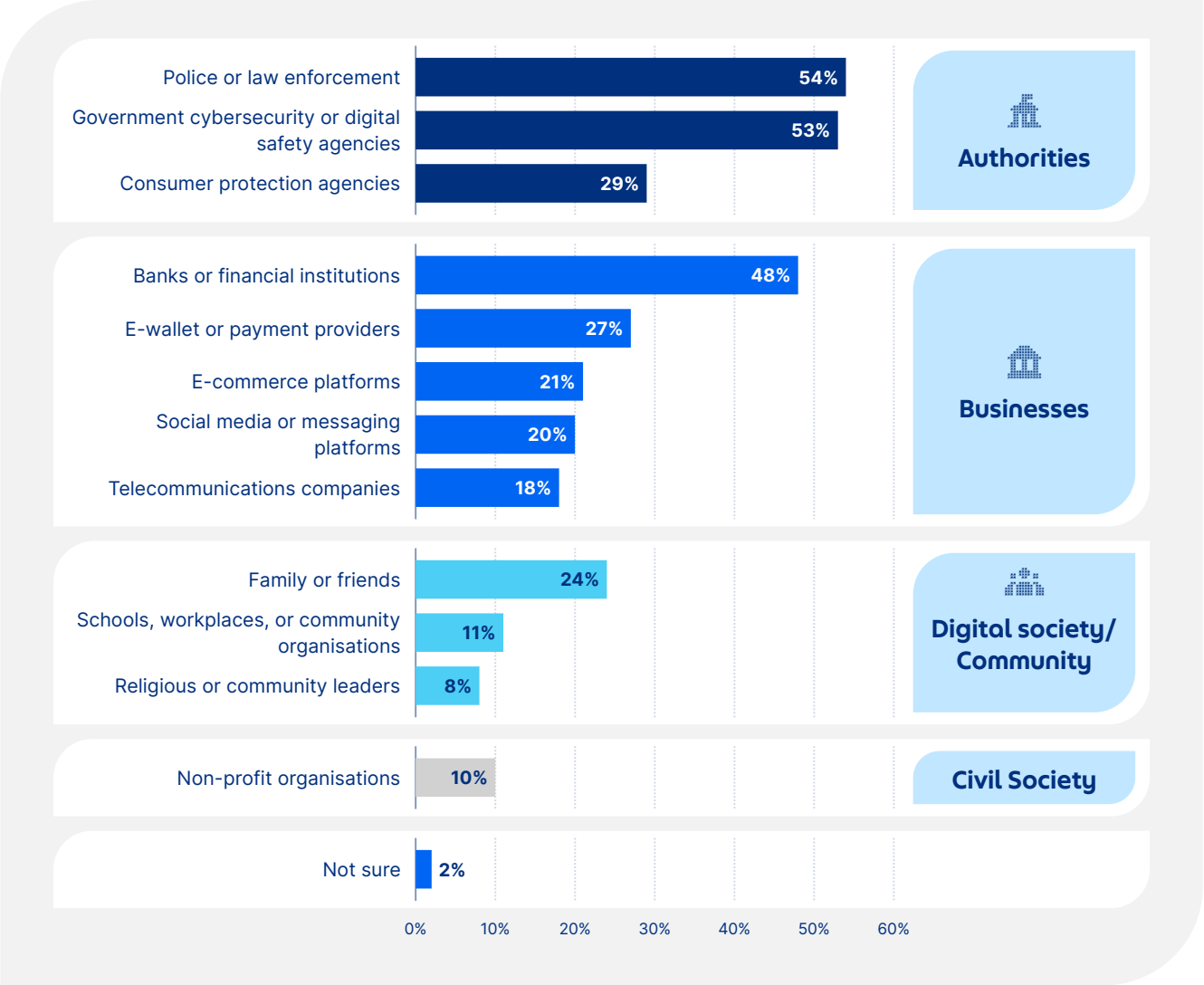


Includes data from the following question: I6. What, if anything, would it take for you to significantly limit your usage of digital goods and services because of scams or fraud?

Source: Tech for Good Institute, 2026

This is where users lean on authorities and financial institutions to mitigate the impact of scams. More than half say they trust law enforcement and government agencies to respond to a scam attempt. But this trust may not always lead to practical action. Despite users turning to institutions to ensure their online safety, the lack of reporting clarity may indicate either an unwillingness or inability to reach them during an actual incident. Southeast Asians also look to their communities for assistance in a different capacity. While institutions are the first port of call after a scam has occurred, family, friends and local organisations still play a role in supporting victims in the aftermath.

Figure 13. Institutional Trust to Respond To Scams



Includes data from the following question: G4. Which of the following organisations or groups would you trust to help you respond to scams or fraud?

Source: Tech for Good Institute, 2026

Tangible improvements to security measures form the gateway to trust in digital systems. Users look for stronger identity verification, faster response from institutions, and increased vigilance in platform screening of risky accounts and transactions. While these are the clear priorities, providing support to victims is no less important.

However, trust is not always so easily restored. For a minority (2%), there is nothing that can restore their trust once lost. While the disengagement of this subset of users may not seem like much, the broader picture is still that trust is conditional. It is contingent on users feeling that there is substantial work being done to ensure their safety. And while they may depend on institutions for protection, 43% still feel they are left to handle scam risks on their own.

Figure 14. Methods to Restore and Strengthen Trust in Digital Services After Falling for Scams



Includes data from the following question: I3. What would help restore or strengthen your trust in digital services after scam or fraud concerns?

Source: Tech for Good Institute, 2026

Scam resilience is underpinned by sustainable and adaptive trust infrastructure. Users clearly seek the signposts that assure them they are safe. This can range from sophisticated verification mechanisms to timely prompts and warnings. More importantly, anti-scam measures should be adaptive: able to continuously adjust to the evolving scam landscape and incorporate user feedback. This requires institutions to remain agile and collaborative, legal and regulatory mechanisms to be responsive, and all of society to be willing to share the burden of online safety.



3. Policy Recommendations

Realising scam resilience in Southeast Asia is a work in progress. While many have grown familiar with commonly known schemes, these skills and knowledge are not necessarily transferable. The emergence of new types and presentations of scams, and the subsequent uncertainty of those who encounter them, indicate that programmes cannot remain static. As scams evolve, so should the measures that aim to mitigate them.

This chapter presents an overview of the policy implications from the findings and an initial set of recommendations to address them. Solutions may apply throughout the entire scam lifecycle (before, during, after, or long term) or to specific stages only. Examples of how initiatives under each recommendation can incorporate a whole-of-society approach are also provided. Such an approach is based on the principle that no single entity can effectively tackle scams alone,[30] and considers five stakeholder groups: governments, businesses, civil society organisations, community networks, and end-users. The figure below provides examples of the entities that might belong to each group:

Figure 15. Expanding on the Whole-of-Society Approach



Source: Tech for Good Institute, 2025

Opportunities for regional coordination exist at every phase. While the report recognises that each country's scam landscape is unique, recommendations are developed from a regional lens. They provide a starting point for countries to localise initiatives to fit their context, and anchor on areas where cooperation across Southeast Asia strengthens national programmes.

3.1 Protect Universally

The findings indicate that scam exposure is now a feature of digital participation. It is no longer a risk confined to conventionally vulnerable groups. As such, protection measures should be designed to be universal in scope – not as one-size-fits-all, but rather with thoughtful consideration of how applicable each one may be to different groups and traits.

Protecting universally can begin with:

- **Ensuring the overall anti-scam strategy is inclusive and culturally aware,** tailoring initiatives to meet the needs of different population segments. This includes understanding the specific challenges encountered by each segment and the most suitable channels and formats for interventions. Building the evidence base may involve consolidating scam cases in a single dataset and leveraging the expertise of different sectors.

- **Facilitating baseline scam literacy.** The data shows that 23% of the population have not received any form of scam training. Of those who have, 25% did not particularly find the training useful. Further, whether the training results in improved detection and response skills is uncertain. Learnings from the scam encounters of various segments can help to determine what the real gaps in scam knowledge are. In turn, this can be used by the relevant governing body to define what baseline scam literacy should look like, including the skills that need to be developed and how. The design and delivery of the curriculum can then be further customised to the target audience.

3.2 Verify Routinely

It is important that users are able to detect scam attempts based on clear markers rather than on personal feelings. The risk of relying on vigilance alone is that it does not fully guard against instances where the cues are seemingly legitimate. At the same time, it can hinder genuine digital engagement.

Developing the evidence-based ability to intercept a scam attempt is honed over time. Scam identification skills, as seen from the data, are not necessarily transferable: scams vary in how they present, and previous exposure does not necessarily lead to better outcomes. Additionally, scams today are rarely static stimuli. In recent years, they have involved longer periods of engagement combined with more advanced ways of faking authenticity. A user's ability to verify whether a transaction is genuine will need to evolve continuously, ideally enabled by other participants in the ecosystem, and done as part of their digital routine.

Verifying routinely may be enabled by:

- **Development of lifelong scam training pathways.** According to survey results, 89% of scam victims have actually received some form of scam training. But there is a gap in identification skills between them and non-victims, despite the latter having slightly less exposure to different forms of scam training. The relevant governing body should thus seek to understand and address this gap in the design and implementation of scam training pathways. A hypothesis is that scam victims may rely on alerts and warnings without understanding why they appear. In fact, 40% of victims believe real scam examples and case studies are more useful forms of training, along with in-app warnings or tips during transactions (38%). Lifelong scam training should thus prioritise teaching critical thinking and other soft skills to complement existing security measures. This includes, but is not limited to: learning to pause before acting, corroborating information through official sources, and staying updated on how different schemes present. Users can then build on these skills when learning how to verify in practice, such as being able to spot the differences between an official communications channel and a fake one.

- **Enhanced, instructive and ecosystem-led online safeguards.** To help users incorporate the verification of transactions and interactions as part of their digital routine, the digital ecosystem (e.g., key actors such as digital platforms, telcos, financial institutions and law enforcement) will need to be intentional in the design of online safeguards. Online safeguards can have multiple roles: primarily in preventing scams and secondarily in teaching users how to spot them. For the first, the volume of suspicious communications received through phone calls and SMS is clearly a concern, potentially stemming from compromised information online. Cybersecurity and data protection operations should thus be more proactive in tracking data and account breaches, notifying affected users, and exploring solutions to prevent such breaches. For the second, those designing interventions can consider employing behavioural science, experimentation, and user feedback in their process. The goal of combining different methods is to understand which purpose each intervention serves, how to frame them to support user learning, and where best to place them during a transaction or interaction.

3.3 Respond Collectively

Mitigating the impact of a scam when it succeeds starts with a clear response plan and ends with supportive pathways for victim recovery. As discussed earlier in the report, many users in the region unknowingly take risky actions. It is thus important to reinforce their knowledge and execution of the steps that prevent further losses. Response plans are conceptualised on two levels: at the societal level, relating to the efforts of institutions (e.g., banks, telcos, government agencies) and wider communities; and at the individual level, what users can do when a scam has occurred. These are further complemented by societal measures for victim support and recovery, ensuring that victims are assisted through the resolution of their trauma.

There are many ways for societies to *respond collectively* to scams, but initial efforts can include:

- **Developing a common, rehearsed, and accessible scam response playbook.** Such a playbook details the responsibilities of the different stakeholder groups in responding to scams, the societal response plans that are in place, and the specific actions users then need to take after a loss occurs to protect themselves and others. Prior to this, the relevant governing body needs to ensure the timely coordination and consistent implementation of societal scam response mechanisms. At present, survey results imply a seeming disconnect between what users expect of said mechanisms versus what they experience, such as the lack of reporting clarity. Enshrining measures that are ineffective or inconsistently delivered only creates confusion, forcing users to carry the burden of response alone. Reliable scam response plans allow users to focus on the aspects that are most relevant and actionable for them. For example, instead of users having to spend time figuring out where to report cases, a common scam response playbook can outline for users the reporting channels that are active and responsive. It can also detail other protective actions that are available on the platforms used during the scam attempt, such as options to block, verify if an account is genuine, or apply for the retrieval of funds.

- **Championing a holistic approach to victim support and recovery.** An empowering environment for victims is built on the key principles of transparency and the preservation of dignity. Victims should have access to information regarding the progress and resolution of their case, including the possibility for redress and other assistance provided. Supportive measures help to address psychosocial effects through empathetic reporting channels and escalation protocols, legal and financial assistance where applicable, and access to mental health support services. Beyond this, work is still needed to create spaces where victims feel safe, heard, and free of judgement or blame. An example is the conscious framing of scam awareness campaigns and related communications to emphasise the actions of the scammer rather than the victim. Complementing this is the availability of professional and trauma-informed care to assist victims in processing the incident and not taking on the burden of blame. Ultimately, individuals need to make a conscious effort to recognise their tendency to victim-blame and shift their thinking whenever they lapse into doing so.

3.4 Trust Confidently

Long-term efforts should focus on sustaining trust in digital systems. As the data shows, digital participation hinges on users feeling like their accounts are protected and serious measures are being taken to address scams. Additionally, the loss of trust can only be partially attributed to the occurrence of the scam itself. Users indicate that the quality of scam response and measures for recovery matter a great deal in winning back trust. In practice, this involves the continuous improvement of policies, tools, and implementation throughout the scam lifecycle.

Empowering users to *trust confidently* is a concerted effort, which may at first look like:

- **Continued investment in strengthening trust infrastructure.** Trust is built through consistent, tangible proof of safety and security. The foregoing definition of digital trust is the demonstrable capability of an organisation to ensure its digital systems and services operate securely, reliably, and accountably, aligned to recognised standards and real-world requirements.[31] It encompasses, among others, privacy, data protection, and governance.[32] This is evident in survey respondents prioritising concrete solutions such as stronger identity verification and account screening processes, above intangibles like community support.
- **Building adaptive capacity for scam resilience.** Previous stakeholder conversations have identified opportunities to update legal and regulatory systems, scale up anti-scam solutions, and orient regional cooperation efforts around scams to be more proactive and future-ready.[33] This entails a mindset shift, investment in implementation capabilities, and having an updated view on how scam strategies should evolve. One way to do so is by leveraging the region's collective expertise through initiatives like the ASEAN Guide on Anti-Scam Policies and Best Practices.[34] Systems will also need to be agile, potentially relying on automation and predictive intelligence to detect patterns from newly reported scam cases to adjust thresholds for detection. More importantly, collaborations among the different stakeholder groups can help to ensure anti-scam policies adequately identify and address the gaps in protection.

The following section provides examples of how high-level recommendations can be translated into specific initiatives, and further, into the ways that different stakeholder groups can contribute to realising each initiative.

3.5 Translating Recommendations into Initiatives

The table below illustrates a sample initiative for each recommendation and the role that each stakeholder group plays. Recommendations and sample initiatives are provided at the first level and can be fleshed out in greater detail, accounting for country nuances and in collaboration with the relevant national stakeholders.

Implication	Recommendation	Sample Initiative	Government	Businesses	Civil Society Organisations	Community Networks	End-Users
Protect Universally	**Design an inclusive and culturally aware overall anti-scam strategy**	Build and maintain a consolidated scam database (suspected and confirmed cases) to provide inputs for the anti-scam strategy development	↗ Designate the governing body to lead the effort ↗ Fund the required resources and capabilities for implementation	↗ Contribute resources and capabilities in data management and analytics ↗ Build and maintain own database for reported scam cases on own platforms	↗ Contribute anecdotal evidence from vulnerable groups ↗ Lead community campaigns to report scam cases	↗ Advocate for scam case reporting in local communities ↗ Support community members in navigating reporting tools and platforms	Understand and use the tools and platforms to report scam cases

Implication	Recommendation	Sample Initiative	Government	Businesses	Civil Society Organisations	Community Networks	End-Users
Protect Universally	**Facilitate baseline scam literacy**	Tailor scam education efforts to different population segments (e.g., demographic groups, scam detection personas, or as deemed relevant to the scam landscape)	↗ Designate the governing body to lead the effort ↗ Define the target population segments and addressable gaps in scam education per segment ↗ Design the reference curriculum according to the definition of baseline scam literacy, consolidating recommendations from different sectors ↗ Provide guidelines for how different sectors can support implementation, including which segments and needs their specific efforts address	↗ Tailor scam education efforts to users/clients, including developing the appropriate formats and content for the relevant segments within the platform (as defined by government) ↗ Share knowledge and best practices within and across sectors for effective channels and formats in platform-led scam training	Support the government in tailoring scam education efforts, especially for vulnerable groups, by contributing community evidence and research	↗ Support the government in implementing scam education efforts at the local community level ↗ Train and activate local educators and peer support groups for the delivery of scam education modules within the community	↗ Participate in scam education efforts ↗ Apply learnings in daily life and business operations

Implication	Recommendation	Sample Initiative	Government	Businesses	Civil Society Organisations	Community Networks	End-Users
Verify Routinely	**Development of lifelong scam training pathways**	Design scenario-based scam training modules	↗ Create a scam skills taxonomy as basis for the training modules ↗ Continuously develop and implement scenario-based training modules according to target outcomes (e.g., skills developed, scam types addressed) ↗ Incentivise partnerships between sectors in delivering scenario-based scam training	↗ Coordinate with the government in the design of scenario-based training modules, drawing on platform data on scams ↗ Deploy scenario-based training modules relevant to platform users (e.g., short in-app videos) or within organisation (e.g., phishing email simulations)	↗ Coordinate with the government in the design of scenario-based training modules, drawing on evidence from research and consultations with users ↗ Deploy scenario-based scam training relevant to members	↗ Drive community-led scenario-based scam training aligned with government requirements ↗ Help to translate learnings from scam training into safe digital practices for community members	↗ Participate in scenario-based scam training ↗ Understand how learnings from scam training apply in practice ↗ Incorporate learnings in the daily verification of digital transactions

Implication	Recommendation	Sample Initiative	Government	Businesses	Civil Society Organisations	Community Networks	End-Users
Verify Routinely	**Enhanced, instructive and ecosystem-led online safeguards**	Continuously enhance anti-scam tools and measures	↗ Consolidate best practices and encourage cross-sectoral sharing of replicable anti-scam tools and measures ↗ Incentivise the upgrade of anti-scam tools and measures across the digital ecosystem ↗ Continuously update and share guidelines on the design of anti-scam tools and measures, based on user feedback and insights from reported scam cases	↗ Collaborate with other sectors in innovating anti-scam tools and measures ↗ Continuously research and update the implementation of anti-scam tools and measures ↗ Offer low-cost anti-scam tools to other organisations that lack security capabilities	↗ Advocate for inclusive, rights-based anti-scam tools and measures ↗ Independently gather feedback (effectiveness, usability, inclusivity) on anti-scam tools and measures ↗ Collaborate with government in diagnosing gaps in anti-scam tools and measures	↗ Act as focal point for community concerns about anti-scam tools and measures ↗ Host local programmes for teaching community members on the use of anti-scam tools on digital platforms	↗ Provide feedback and report scam attempts to help inform the design of anti-scam tools and measures ↗ Stay updated on the latest anti-scam tools and measures ↗ Share protective knowledge (e.g., available anti-scam tools and ways of verification) with family and friends

Implication	Recommendation	Sample Initiative	Government	Businesses	Civil Society Organisations	Community Networks	End-Users
Respond Collectively	**Developing a common, rehearsed and accessible scam response playbook**	Ensure the timely and consistent implementation of societal scam response mechanisms	↗ Set and enforce standards for scam response (e.g., speed, efficiency, quality of resolution) ↗ Coordinate scam response efforts, ideally through a designated, inter-agency governing and implementing body ↗ Lead the development of a common scam response playbook for users	↗ Comply with standards for scam response (e.g., speed, efficiency, quality of resolution) ↗ Participate in coordinated scam response efforts ↗ Enhance in-platform transaction controls (e.g., account blocking/freezing)	↗ Collect data from user experiences on whether scam response is compliant with standards ↗ Educate communities on the societal scam response mechanisms available	↗ Serve as local escalation points for cases or concerns on the enforcement of scam response standards ↗ Reinforce knowledge of societal scam response mechanisms and standards	Share perspective on the effectiveness, timeliness and reliability of societal scam response mechanisms

Implication	Recommendation	Sample Initiative	Government	Businesses	Civil Society Organisations	Community Networks	End-Users
Respond Collectively	**Championing a holistic approach to victim support and recovery**	Facilitate a blame-free culture through scam awareness campaigns	↗ Establish guidelines for appropriate, non-judgemental language and framing of scam awareness campaigns ↗ Lead the design and implementation of blame-free scam awareness campaigns	Develop and launch neutral, non-judgemental scam awareness campaigns according to government guidelines	Advocate for inclusive and non-judgemental scam awareness campaigns	Host community-based forums or informal talks on destigmatising victimhood	Contribute to destigmatisation efforts through sharing experiences in safe spaces (e.g., trusted social circles, inclusive and culturally sensitive community-based forums)

Implication	Recommendation	Sample Initiative	Government	Businesses	Civil Society Organisations	Community Networks	End-Users
Trust Confidently	**Continued investment in strengthening trust infrastructure**	Design and implement guidelines for stronger national and institutional trust infrastructure	↗ Fund initiatives for building national trust infrastructure (e.g., enhancing enforcement capacity) ↗ Establish guidelines for national and institutional trust infrastructure (i.e., the breadth and depth of security and data protection measures on platforms or within organisations)	Invest in stronger institutional trust infrastructure (e.g., strengthening identity verification checks), based on government guidelines	Contribute research and evidence for designing institutional trust infrastructure guidelines	Gather and share community perspectives on specific areas of the trust infrastructure (e.g., effectiveness of current transaction authorisation practices)	Participate in simulations and user testing of anti-scam solutions developed based on the latest trust infrastructure guidelines

Implication	Recommendation	Sample Initiative	Government	Businesses	Civil Society Organisations	Community Networks	End-Users
Trust Confidently	**Building adaptive capacity for scam resilience**	Develop the capability to continuously innovate anti-scam policies and tools	↗ Invest in instruments for anti-scam policy and tool innovation (e.g., sandboxes) ↗ Collaborate with other sectors of society to develop advanced anti-scam solutions	↗ Participate in anti-scam policy and tool innovation (e.g., sandboxes) ↗ Share the latest knowledge on resources and capabilities needed for innovating anti-scam policies and tools	Support research and evidence gathering to inform the design of new anti-scam policies and tools	↗ Advocate for innovation in anti-scam policies and tools to address community challenges ↗ Serve as a bridge between community evidence, empirical research, and policy to innovate anti-scam tools	Share individual experiences to improve future anti-scam policy and tool innovation



TECH FOR GOOD INSTITUTE

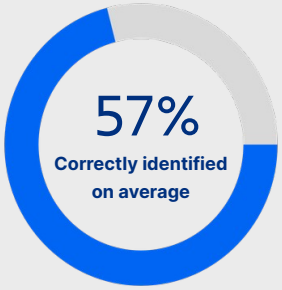
Appendix A. Spot-the-Scam Scorecard

THE SPOT-THE-SCAM SCORECARD

How well did consumers identify seven scenarios across Southeast Asia?

Consumers correctly identified scams 71% of the time, but performance varies considerably by scenario and country.

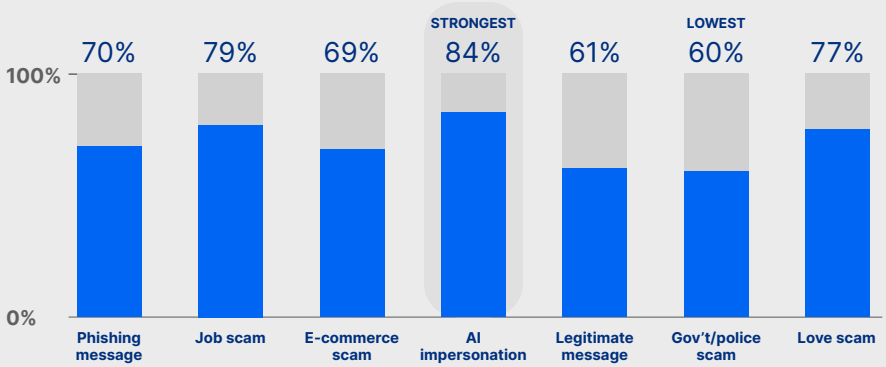
OVERALL IDENTIFICATION



Average across seven scam tests

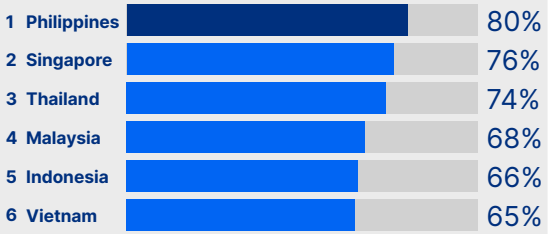
29% did not identify the scam

SEVEN-TEST SCORECARD



A 24-point gap separates the easiest and hardest scenarios.

AVERAGE BY COUNTRY

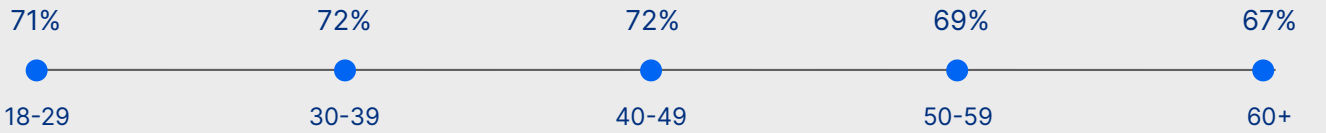


LARGEST DIVIDE: LEGITIMATE MESSAGE
Philippines 87% vs Malaysia 36%

51-point gap

AGE DIFFERENCES ARE SMALLER

Market and scenario differences are more pronounced than age differences.



60+ base: n=235

KEY TAKEAWAY

Scam awareness is relatively strong overall, but two scenarios expose clear blind spots - and the ability to spot them differs sharply by country.

Vulnerability is concentrated, not uniform

The scorecard combines scenario-level detection with country and age comparisons to show where strong overall awareness masks specific blind spots.

Source: Tech for Good Institute, Scams and Fraud Study, 2026. Total n=6,000; country samples n=1,000 each. Figures show the percentage correctly identifying each stimulus; country and age scores are averages across seven stimuli.



TECH FOR GOOD INSTITUTE

Appendix B. Country Highlights

This section provides highlights of each country's performance.

Where the regional findings reveal a common scam-resilience challenge, expression differs considerably across Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam.

The highlights examine how exposure, confidence, response readiness and trust come together within each market. They are intended to show the nuances beyond the regional average and cannot and should not be taken as a ranking of each market on any measure.

Indonesia

Indonesia's scam exposure tracks the regional average, but conversion is high: 49% report losing something of value. Concern is correspondingly elevated, leading to heightened vigilance as the main driver of Indonesians' confidence in detecting scams. Improving response readiness is thus a priority.

Snapshot/Overview



Figure ID-1. Exposure, victimisation, concern and scam-readiness personas.

Top Factors Shaping Confidence

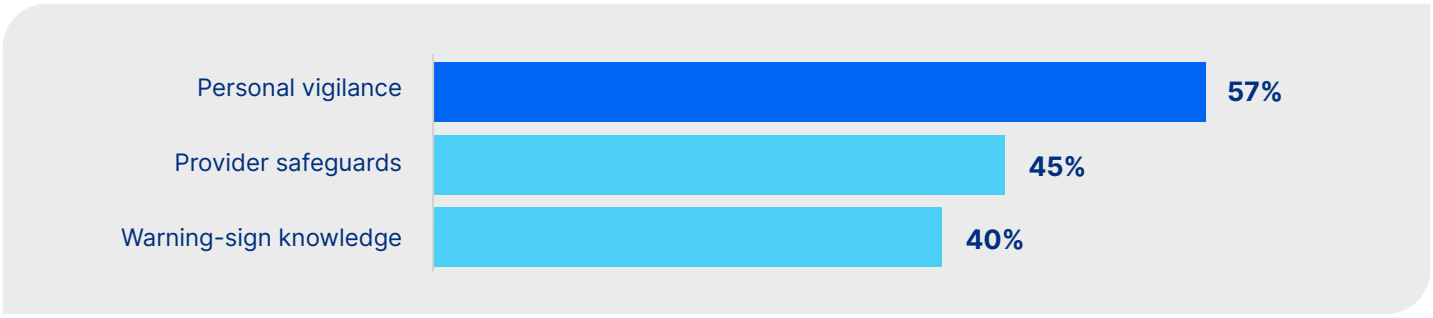


Figure ID-3. Confidence gap and leading confidence factors.

Post-loss Response And Recovery Needs

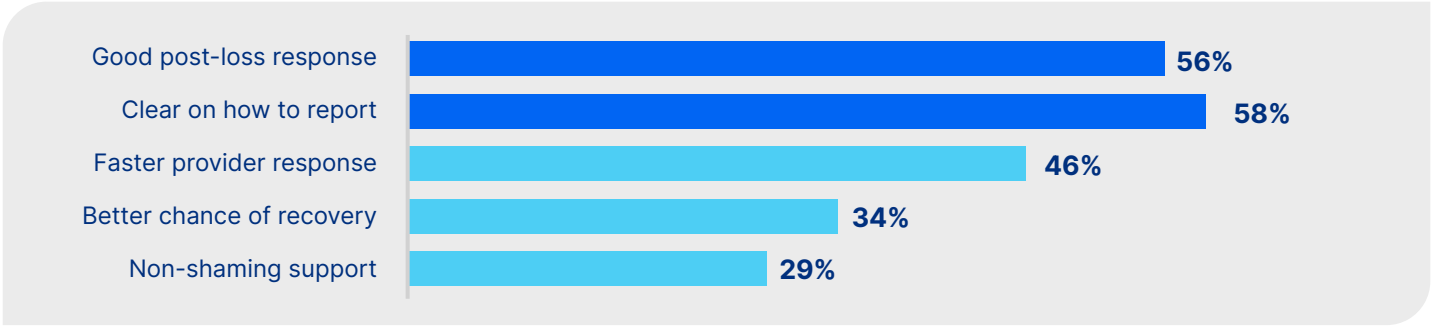


Figure ID-5. Post-loss capability, impact and recovery priorities.

Institutional Trust And Restoration



Figure ID-7. Trusted institutions and actions most likely to restore trust.

Regional finding: Gender and education do not meaningfully distinguish scam victimisation, while age and economic activity primarily shape exposure through greater digital participation

Source: Tech for Good Institute, Scams and Fraud Study, 2026. n=1,000 per country. Percentages rounded.

Malaysia

Malaysia's exposure profile, including conversion to loss and degree of concern, sits close to the regional average. Alongside personal vigilance, their confidence is influenced by government-led awareness campaigns. However, reporting clarity sits below regional average, suggesting uncertainty about official communications that needs to be addressed.

Snapshot/Overview



Figure MY-1. Exposure, victimisation, concern and scam-readiness personas.

Top Factors Shaping Confidence

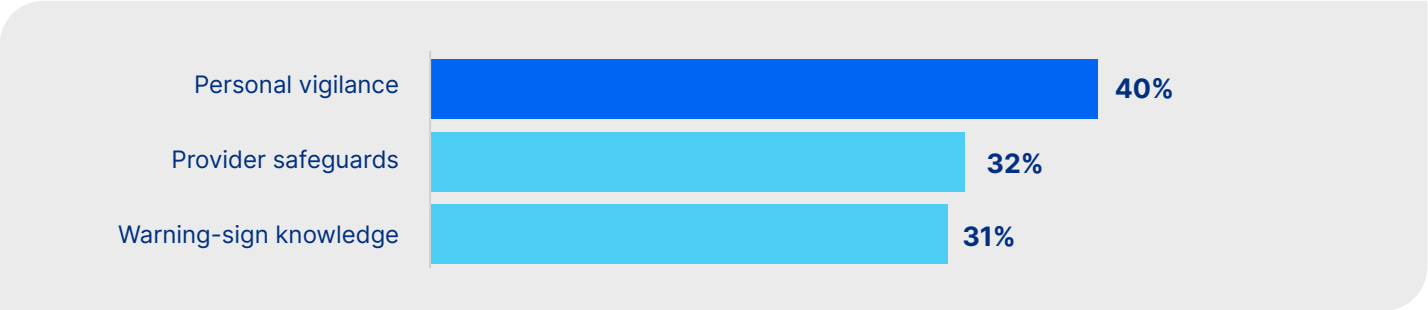


Figure MY-3. Confidence gap and leading confidence factors.

Post-loss Response And Recovery Needs

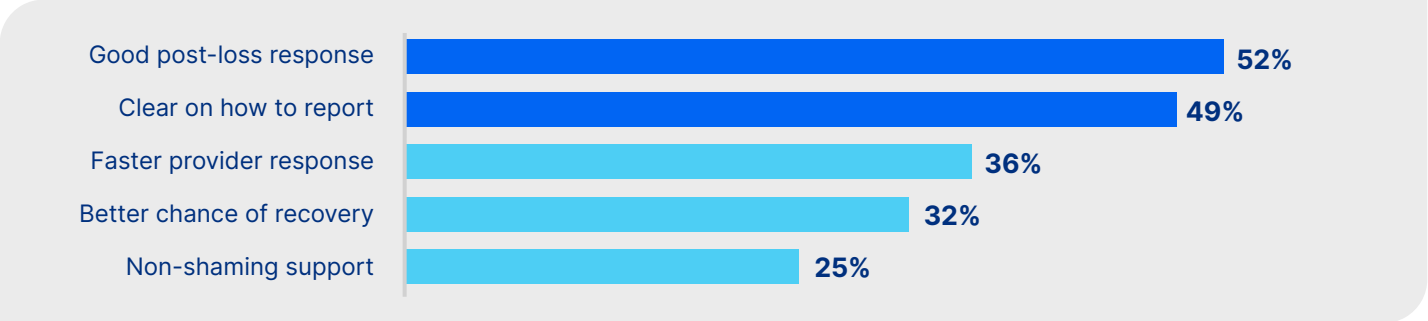


Figure MY-5. Post-loss capability, impact and recovery priorities.

Institutional Trust And Restoration



Figure MY-7. Trusted institutions and actions most likely to restore trust.

Regional finding: Gender and education do not meaningfully distinguish scam victimisation, while age and economic activity primarily shape exposure through greater digital participation

Source: Tech for Good Institute, Scams and Fraud Study, 2026. n=1,000 per country. Percentages rounded.

Philippines

The Philippines records higher exposure, conversion to loss, and significantly elevated concerns regarding scams compared to the regional average. Vigilance is heightened and complemented by knowledge and verification practices. Awareness is no longer an issue, but there remain gaps in post-loss response and preventive measures.

Snapshot/Overview



Figure PH-1. Exposure, victimisation, concern and scam-readiness personas.

Top Factors Shaping Confidence

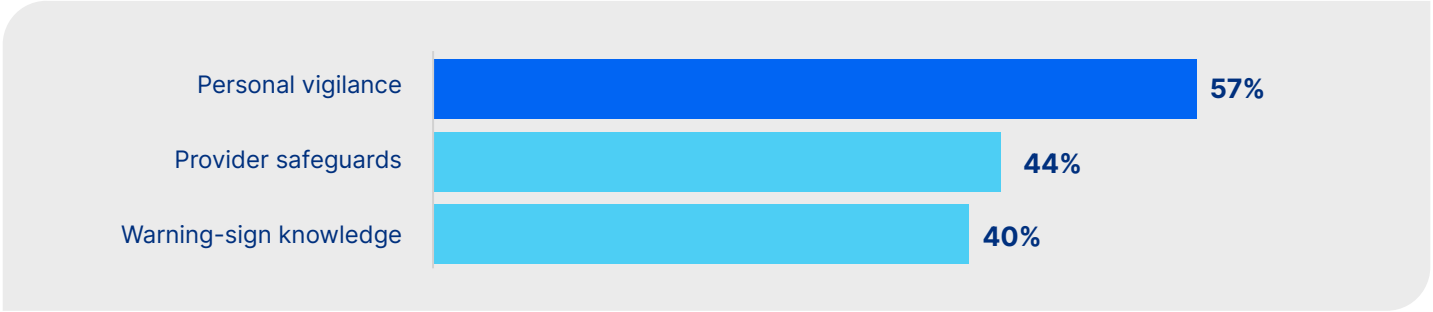


Figure PH-3. Confidence gap and leading confidence factors.

Post-loss Response And Recovery Needs

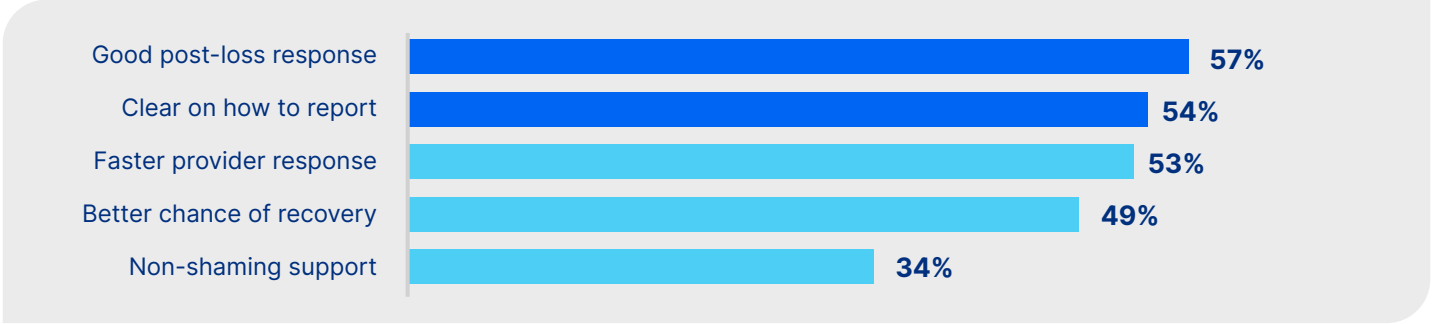


Figure PH-5. Post-loss capability, impact and recovery priorities.

Institutional Trust And Restoration



Figure PH-7. Trusted institutions and actions most likely to restore trust.

Regional finding: Gender and education do not meaningfully distinguish scam victimisation, while age and economic activity primarily shape exposure through greater digital participation

Source: Tech for Good Institute, Scams and Fraud Study, 2026. n=1,000 per country. Percentages rounded.

Singapore

Singapore records the lowest exposure and concern rates in the region. More of them tend to take safe actions in response to a loss, but unusually demonstrate more confusion about where to report cases. This is despite high institutional trust. Closing the loop is the concern for this nation: improving recovery mechanisms and clarity of reporting channels.

Snapshot/Overview



Figure SG-1. Exposure, victimisation, concern and scam-readiness personas.

Top Factors Shaping Confidence

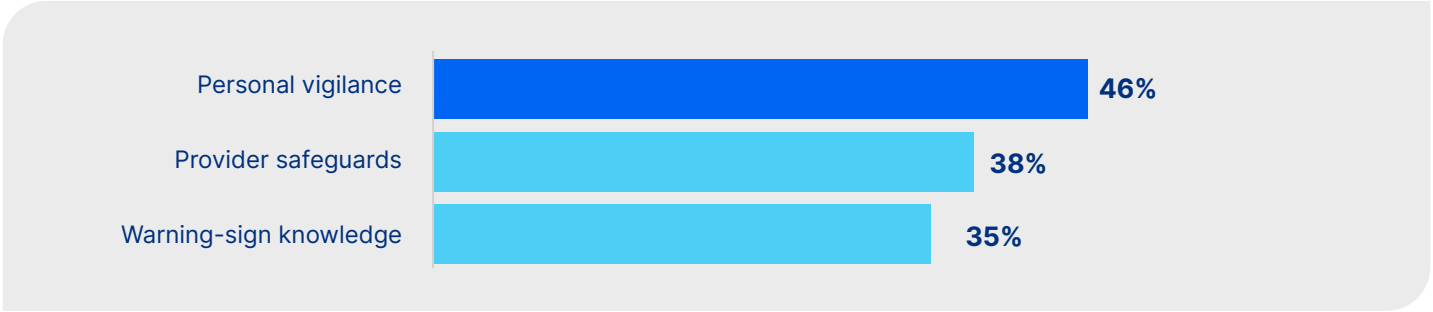


Figure SG-3. Confidence gap and leading confidence factors.

Post-loss Response And Recovery Needs

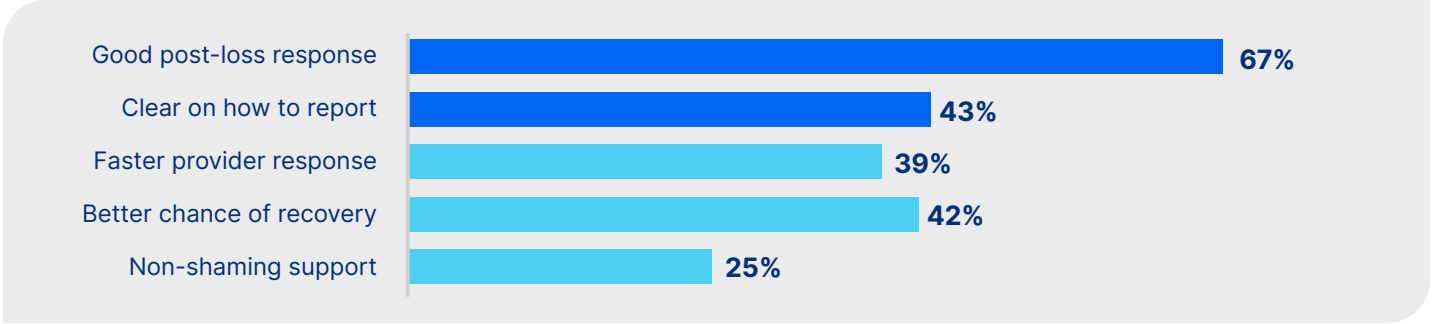


Figure SG-5. Post-loss capability, impact and recovery priorities.

Institutional Trust And Restoration



Figure SG-7. Trusted institutions and actions most likely to restore trust.

Regional finding: Gender and education do not meaningfully distinguish scam victimisation, while age and economic activity primarily shape exposure through greater digital participation

Source: Tech for Good Institute, Scams and Fraud Study, 2026. n=1,000 per country. Percentages rounded.

Thailand

Thailand has among the highest levels of scam exposure but comparatively low victimisation and the region's lowest concern. Response capability is relatively strong, suggesting that the priority is to preserve operational readiness while preventing familiarity with scams from turning into complacency.

Snapshot/Overview



Figure TH-1. Exposure, victimisation, concern and scam-readiness personas.

Top Factors Shaping Confidence

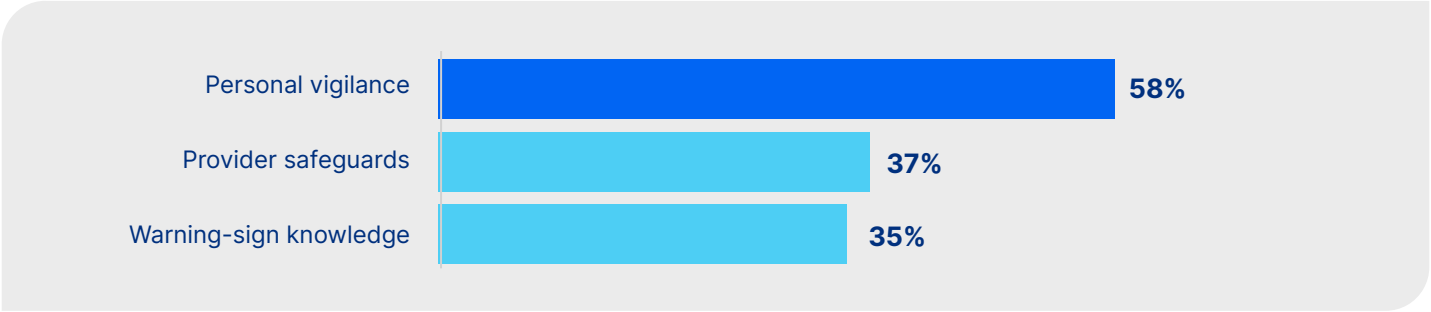


Figure TH-3. Confidence gap and leading confidence factors.

Post-loss Response And Recovery Needs

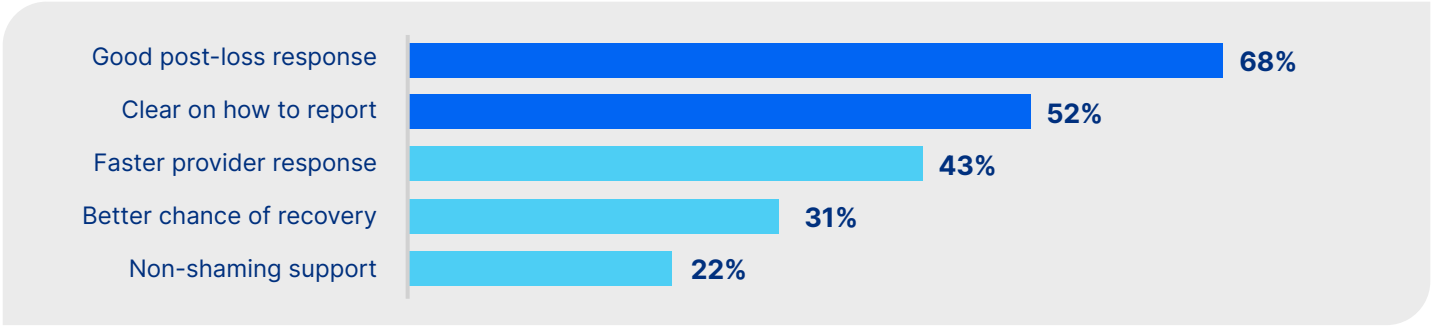


Figure TH-5. Post-loss capability, impact and recovery priorities.

Institutional Trust And Restoration



Figure TH-7. Trusted institutions and actions most likely to restore trust.

Regional finding: Gender and education do not meaningfully distinguish scam victimisation, while age and economic activity primarily shape exposure through greater digital participation

Source: Tech for Good Institute, Scams and Fraud Study, 2026. n=1,000 per country. Percentages rounded.

Vietnam

Vietnam's exposure and conversion to loss sit above the regional average, while concern and personal vigilance are aligned with their peers. They believe AI has raised the difficulty of detecting scams. While they are clear about where to report and demonstrate high institutional trust, there is a gap in individual response readiness.

Snapshot/Overview



Figure VN-1. Exposure, victimisation, concern and scam-readiness personas.

Top Factors Shaping Confidence

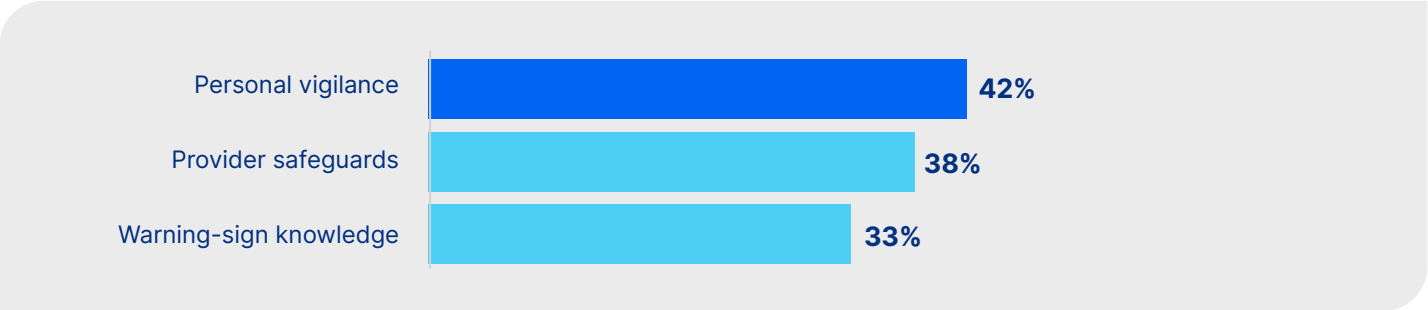


Figure VN-3. Confidence gap and leading confidence factors.

Post-loss Response And Recovery Needs

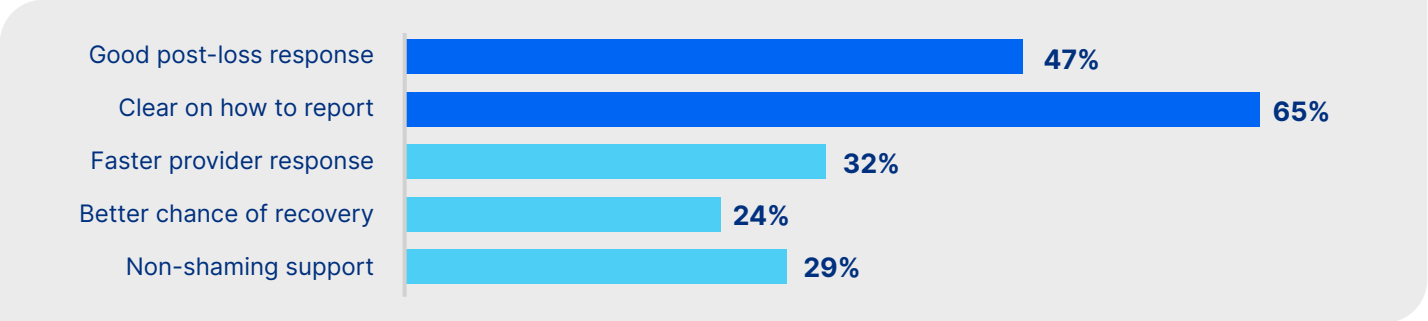


Figure VN-5. Post-loss capability, impact and recovery priorities.

Institutional Trust And Restoration



Figure VN-7. Trusted institutions and actions most likely to restore trust.

Regional finding: Gender and education do not meaningfully distinguish scam victimisation, while age and economic activity primarily shape exposure through greater digital participation

Source: Tech for Good Institute, Scams and Fraud Study, 2026. n=1,000 per country. Percentages rounded.

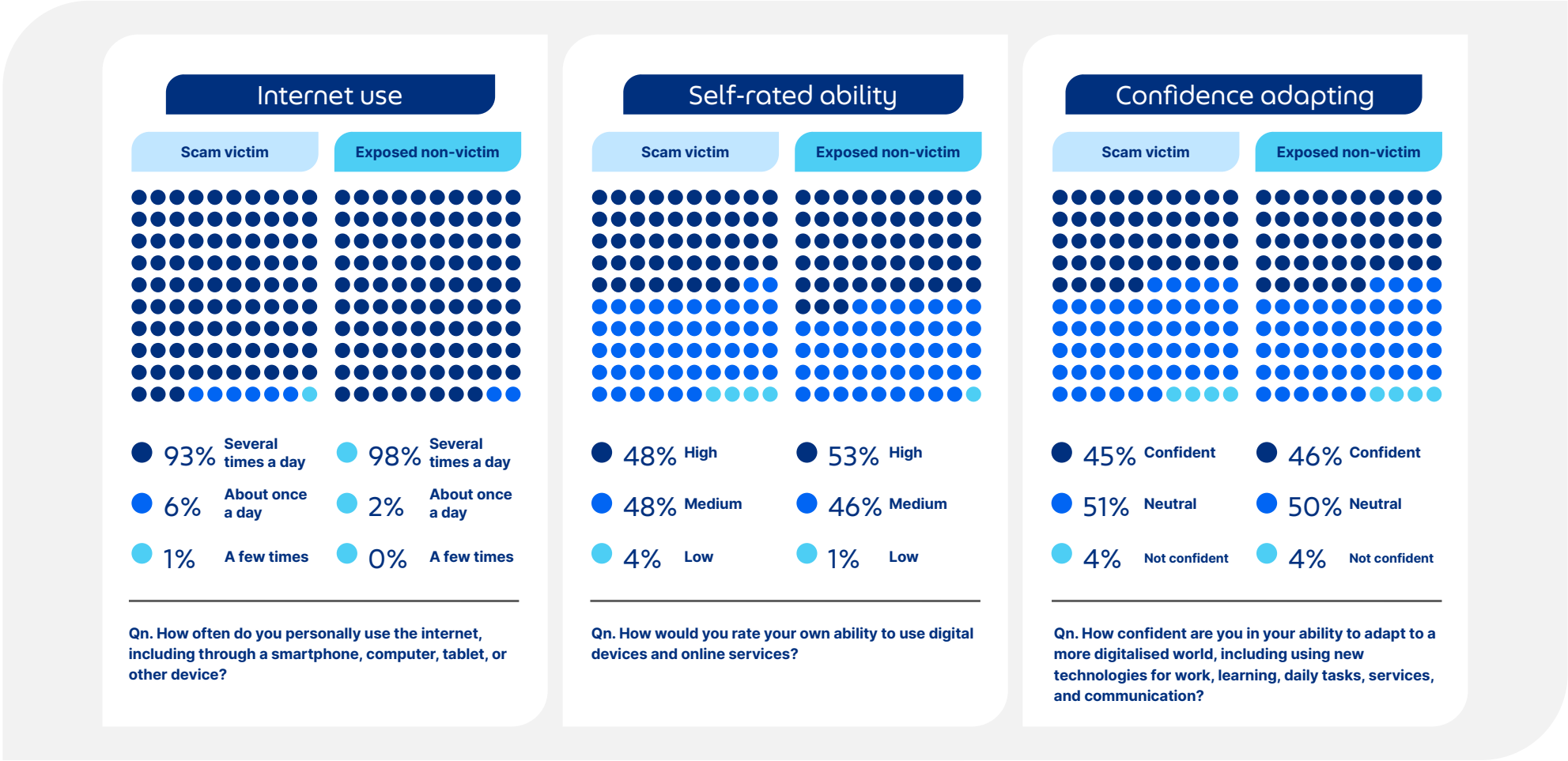


TECH FOR GOOD INSTITUTE

Appendix C. Supplementary Exhibits

C.1 Protect: The Exposure Risk

Exhibit 1. Comparison of digital participation intensity between scam victims and exposed non-victims



Source: Tech for Good Institute, 2026

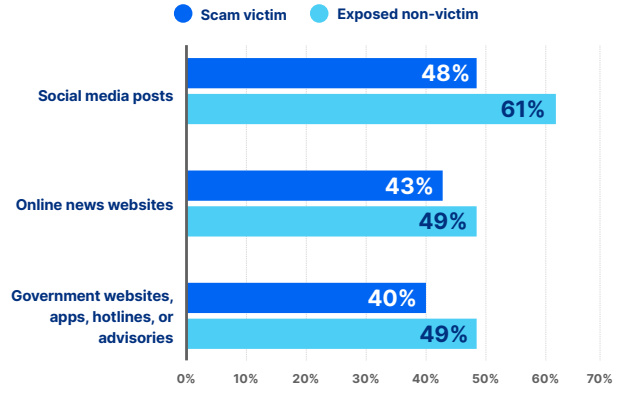
Exhibit 2. The attitudinal differences between victims and exposed non-victims

Attitudinal and Behavioral Profiles: Victims vs. Exposed Non-Victims

Digital Confidence	Scam victim	Exposed non-victim
I feel confident using digital services	66%	61%

Institutional Trust	Scam victim	Exposed non-victim
I trust that digital services are safe for me to use	61%	50%
I trust banks and financial institutions to help users respond to scams and fraud	66%	59%

Information Channels Used to Verify Scams

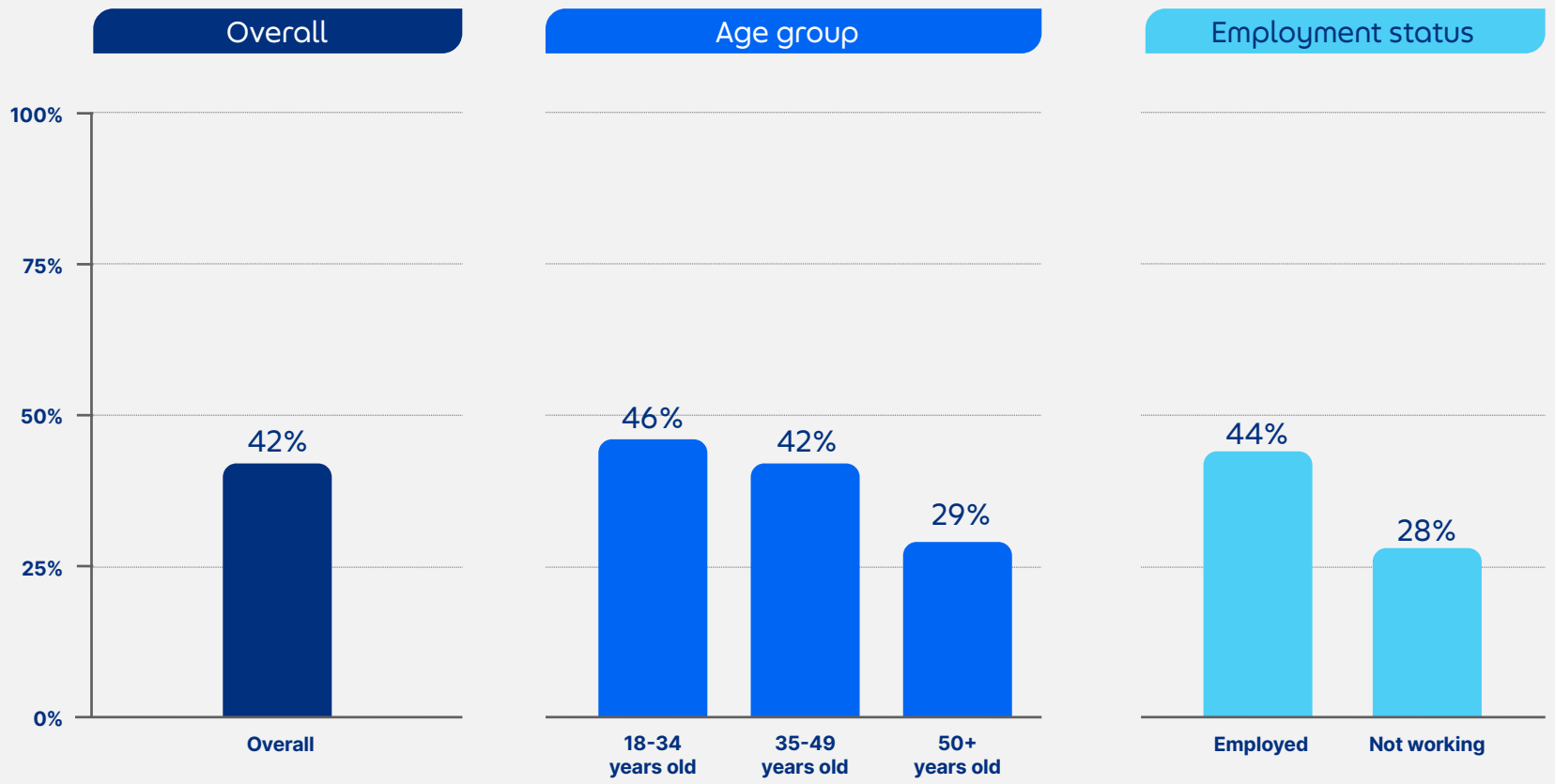


Report and Escalate	Scam victim	Exposed non-victim
Verify through an official website, app, hotline, or physical branch	45%	51%
Report it to the relevant platform, bank, or authority	48%	57%
Active Defence		
Search online to see if others reported something similar	33%	34%
Stop responding to the sender or caller	43%	52%
Block the sender or caller	49%	63%
Ask family or friends for advice	27%	22%
Interrogative Action		
Continue the conversation to gather more proof	25%	15%
Risky Sharing		
Share the suspicious link or phone number with others to warn them	32%	29%
Inaction and Confusion		
Ignore it and do nothing	24%	21%
I would not know what to do	10%	4%

Source: Tech for Good Institute, 2026

C.2 Identify and Detect: The Confidence Trap

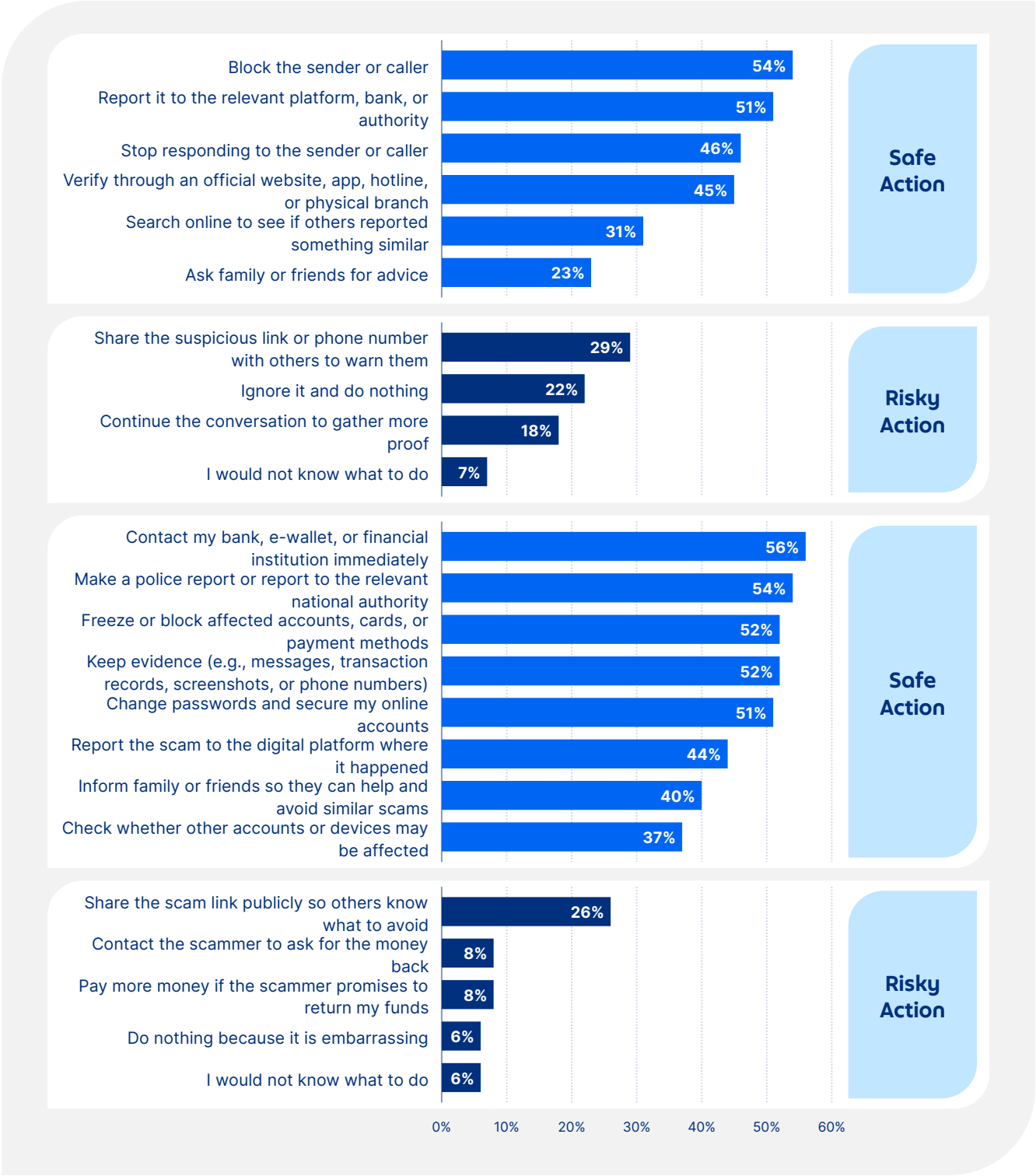
Exhibit 3. Confidence levels by age group and working status



Source: Tech for Good Institute, 2026

C.3 Respond and Recover: The Action Gap

Exhibit 4. Actions taken before and after a scam loss occurs



Source: Tech for Good Institute, 2026

Endnotes and References

Endnotes and References	
1	Tech for Good Institute. (2026, April 24). *Report Launch: Realising a Confident Digital Society: Spotlight on SEA-6*. Retrieved September 1, 2026 from https://web.archive.org/web/20260914045024/https://techforgoodinstitute.org/events/event-highlights/report-launch-realising-a-confident-digital-society-spotlight-on-sea-6/
2	Detros, K. (2025, November 11). *Substantial Conclusion, Substantial Work for ASEAN's Digital Economy Framework Agreement*. Tech for Good Institute. Retrieved September 1, 2026 from https://web.archive.org/web/20260914045242/https://techforgoodinstitute.org/insights/perspectives/substantial-conclusion-substantial-work-for-aseans-digital-economy-framework-agreement/
3	Google, Temasek, & Bain & Co. (2025, November 11). *From Digital Decade to AI Reality: Accelerating the future in ASEAN*. Retrieved September 1, 2026 from https://web.archive.org/web/20260914045131/https://economysea.withgoogle.com/
4	Ibid.
5	Franceschini, I., et al. (2026, April 9). *Southeast Asia's whack-a-mole scam economy. East Asia Forum*. Retrieved August 29, 2026 from https://web.archive.org/web/20261005032738/https://eastasiaforum.org/2026/04/09/southeast-asias-whack-a-mole-scam-economy/
6	The Straits Times. (2026, July 21). *Online scam losses in Asia-Pacific region up to $147 billion in 2025: UN*. Retrieved September 1, 2026 from https://web.archive.org/web/20260914051300/https://www.straitstimes.com/asia/se-asia/scam-losses-in-asian-regions-up-to-147-billion-in-2025-un
7	National Institute for Standards and Technology. (2020). *Glossary: Cyber Resiliency*. Retrieved September 14, 2026 from https://web.archive.org/web/20260914072700/https://csrc.nist.gov/glossary/term/cyber_resiliency
8	Tech for Good Institute. (2025, August 21). *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of- Society Approach*. Retrieved August 29, 2026 from https://web.archive.org/web/20260914051035/https://techforgoodinstitute.org/research/tfgi-reports/building-resilience-against-digitally-enabled-scams-and-fraud-in-southeast-asia-a-whole-of-society-approach/
9	Ibid.
10	Mastercard. (2024, November 26). *Fraud vs. scams: How to spot the difference and stay safe*. Retrieved September 17, 2026 from https://web.archive.org/web/20260917025151/https://www.mastercard.com/global/en/news-and-trends/Insights/2024/fraud-vs-scams-how-to-spot-the-difference-and-stay-safe.html
11	Tech for Good Institute. (2025, August 21). *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of- Society Approach*.
12	Federal Trade Commission. (n.d.). *Phishing scams*. Retrieved June 25, 2025 from https://web.archive.org/web/20250715102925/https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams
13	Federal Trade Commission. (n.d.). *Fake Prize, Sweepstakes, and Lottery Scams*. Retrieved October 9, 2026 from https://web.archive.org/web/20260912214745/https://consumer.ftc.gov/articles/fake-prize-sweepstakes-and-lottery-scams
14	Ibid.

15	ScamWatch. (n.d.). *Impersonation scams.* Retrieved June 25, 2025, from https://web.archive.org/web/20250715103653/https://www.scamwatch.gov.au/types-of-scams/impersonation-scams
16	Federal Trade Commission. (2022, August). *What to know about romance scams*. Retrieved June 25, 2025, from https://web.archive.org/web/20250715104621/https://consumer.ftc.gov/articles/what-know-about-romance-scams
17	ScamWatch. (n.d.). *Jobs and employment scams*. Retrieved June 25, 2025, from https://web.archive.org/web/20250716063616/https://www.scamwatch.gov.au/types-of-scams/jobs-and-employment-scams
18	Scamshield. (2026, May 26). *E-Commerce Scams.* Scamshield. Retrieved August 29, 2026 from https://web.archive.org/web/20260914051535/https://www.scamshield.gov.sg/i-want-protection-from-scams/learn-to-recognise-scams/e-commerce-scams/#322d121465a5d8b517d59dfc7b44f7e8
19	Gusel, L. (2024, December 16). Major regulatory alerts about AI and deepfake fraud signal significant challenge to 2025 digital account growth. Feedzai. Retrieved 25 June 2025 from https://web.archive.org/web/20250715103214/https://www.feedzai.com/blog/fbi-issues-ai-and-deepfake-alert/
20	Erdem, C., Oruç, E., Atar, C. and Bağcı, H. (2023). "The mediating effect of digital literacy in the relationship between media literacy and digital citizenship", Education and Information Technologies, Vol. 28 No. 5, pp. 4875-4891, doi: https://doi.org/10.1007/s10639-022-11354-4.
21	Tech for Good Institute. (2025, August 21). *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of- Society Approach*.
22	Ibid.
23	Tech for Good Institute. (2025, August 21). *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of- Society Approach*.
24	Tech for Good Institute. (2023, May 26). *Towards a Resilient Cyberspace in Southeast Asia*. Retrieved September 14, 2026 from https://web.archive.org/web/20260914072050/https://techforgoodinstitute.org/research/tfgi-reports/towards-a-resilient-cyberspace-in-southeast-asia/
25	Sampling confidence level: Indicates how often the "true" result of a group will fall within the specific range if the survey or test is repeated multiple times.
26	Sampling margin of error (MOE): Indicates how much the survey results might differ from the actual views or behaviours of the population.
27	Tech for Good Institute. (2025, August 21). *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of- Society Approach*.
28	Tech for Good Institute. (2023, May 26). *Towards a Resilient Cyberspace in Southeast Asia*.
29	Tech for Good Institute. (2025, August 21). *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of- Society Approach*.
30	Tech for Good Institute. (2025, August 21). *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of- Society Approach*.
31	CySec Professionals. (n.d.). *What is Digital Trust?* Digital Trust Infrastructure. Retrieved September 11, 2026 from https://web.archive.org/web/20260915084044/https://www.digitaltrust.institute/what-is-digital-trust
32	Tech for Good Institute. (2023, May 26). *Towards a Resilient Cyberspace in Southeast Asia*.

33	Tech for Good Institute. (2025, August 21). *Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of- Society Approach*.
34	Association of Southeast Asian Nations (ASEAN). (2026, January). *ASEAN Guide on Anti-Scam Policies and Best Practices*. Retrieved September 11, 2026 from https://web.archive.org/web/20260914052410/https://asean.org/wp-content/uploads/2026/01/ASEAN-Guide-on- Anti-Scam-Policies-and-Best-Practices-090126.pdf



Tech For Good Institute

www.techforgoodinstitute.org