TECH FOR GOOD INSTITUTE

Report

Building Resilience Against Digitally-enabled Scams and Fraud in Southeast Asia: A Whole-of-Society Approach

September 2025

Supported by

BAMBOO BUILDERS

Google.org

Table of Contents

About This Study

With the aim of strengthening digital resilience across Southeast Asia, this study was undertaken to understand the growing threat posed by online scams and frauds and how it can be mitigated. While awareness of the problem is increasing, there is an opportunity for a regional analysis that brings together perspectives from across sectors to define what digital resilience means in this context, identify the levers for action and clarify the roles and responsibilities of stakeholders.

Specifically, the study examines the evolving landscape of scams and fraud in six Southeast Asian countries: Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam. It aims to define digital resilience in this context, map the lifecycle of scams, and identify practical levers for prevention, disruption and response. It also proposes building digital resilience across the entire scams and fraud lifecycle, with illustrative examples across the region. In addition, this report explores how governments, industry, civil society and academia can work together to strengthen resilience at both national and regional levels.

A qualitative approach was adopted, combining stakeholder engagement with desk-based research. Six virtual multi-stakeholder roundtables were held between April and May 2025, organised in collaboration with convening partners in each of the SEA-6 countries. These dialogues brought together experts from government, industry, civil society and academia to share insights and examples of action. The findings are supported by desktop research and publicly available data.

The report is structured as follows:

- Chapter 1 defines **the problem** through an examination of the increasingly complex threat landscape in Southeast Asia.

- Chapter 2 outlines **who** is essential for a whole-of-society approach to this complex problem.

- Chapter 3 explains **when** interventions should take place and how to target actions across the scam lifecycle.

- Chapter 4 present **examples of action** by different stakeholders as illustrative examples of what is needed to operationalise protection, detection, response and adaptation strategy.

- Chapter 5 outlines **how to sustain** digital resilience, highlighting collaboration, innovation and regional coordination as key to a safer digital future.

Bamboo Builders, Google.org and the Tech For Good Institute intend for this report to be a resource and an invitation to dialogue. We hope that policymakers, regulators, business leaders, researchers and community organisations find this report useful as a starting point for action and collaboration. We welcome feedback, insights and opportunities for partnership. To share your thoughts, please contact info@techforgoodinstitute.org.

Acknowledgements

We appreciate the contributions of more than 70 participants who contributed their time, experience and expertise.* Together, they offer a multi-sectoral and holistic view of stakeholders relevant to this issue, including representatives from ministries, parliaments, telecommunications regulators, law enforcement agencies, educational institutions, think tanks, non-governmental and civic organisations, and companies from the financial, telecommunications, cybersecurity and digital sectors. Their insights, data, and practical recommendations were invaluable to the development of this report. The table below highlights the organisations represented in this study.

🇮🇩 Indonesia	🇲🇾 Malaysia
• Coordinating Ministry for Economic Affairs (Kemenko Perekonomian) • Ministry of Trade (Kemendag) • Ministry of Communications and Digital Affairs (Komdigi) • National Consumer Protection Agency (BPKN) • Financial Services Authority (OJK) • Google • Indonesian Chamber of Commerce (KADIN) • Indonesia Cyber Security and Digitalisation Association (ADIGSI) • Centre for Strategic and International Studies (CSIS) • Center for Indonesian Policy Studies (CIPS) • Southeast Asia Freedom of Expression Network (SAFEnet) • Center for Digital Society (CfDS) • Indonesia Services Dialogue Council	• Cybersecurity Malaysia • Malaysia Digital Economy Corporation (MDEC) • MyDigital • CelcomDigi • AEON Bank Malaysia • Institute of Strategic and International Studies (ISIS) • Malaysia Crime Prevention Foundation • Universiti Malaya • Multimedia University • Universiti Tunku Abdul Rahman

The Philippines

- Bangko Sentral ng Pilipinas (BSP)
- Senate of the Philippines
- Department of Information and Communications Technology (DICT)
- Analytics and Artificial Intelligence Association of the Philippines Government
- Better Than Cash Alliance
- Bankers Association
- Credit Card Association
- Mastercard
- Google
- Globe Telecom
- Gogolook
- BDO Unibank
- Rizal Commercial Banking Corporation (RCBC)
- Global Forum on Cyber Expertise (GCFE)
- Asian Institute of Management (AIM)
- Scamwatch Pilipinas and Truth 360

Singapore

- Ministry of Home Affairs (MHA)
- GovTech Singapore
- Google
- Amazon
- GSMA
- OCBC Bank
- Rajah & Tann Technologies
- ST Engineering
- Association of Certified Anti-Money Laundering Specialists
- Feedzai
- Hong Leong Finance
- Bamboo Builders
- NTU Digital Trust Centre (DTC)
- Lee Kuan Yew School of Public Policy
- S. Rajaratnam School of International Studies (RSIS)

Thailand

- Bank of Thailand (BOT)
- Electronic Transaction Development Agency (ETDA)
- Foundation for Consumers (FCC)
- Thailand Consumers Council (TCC)
- Collaborative Fact Checking (COFACT) Thailand
- Thammasat University

Vietnam

- Central Committee for Policy and Strategy
- Pacific Links Foundation
- FPT Information System
- RMIT University
- Institute for Policy Studies and Media Development (IPS)
- Vietnam Academy of Social Sciences
- Vietnam National University

Note: * Some organisations have requested to remain anonymous.

We also extend our thanks to our convening partners: the Global Anti-Scam Alliance (Singapore and the Philippines), Thailand Consumer Council (Thailand), Centre for Indonesian Policy Studies (Indonesia), Institute of Strategic and International Studies (Malaysia) and Institute of Policy and Strategy (Vietnam). Their critical support and engagement were essential to this initiative.

↗ About the Tech for Good Institute

The Tech for Good Institute is a non-profit organisation 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 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. The Tech for Good Institute 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. The Institute was founded by 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.

Funders do not determine research findings nor the insights and recommendations of research.

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

↗ About Bamboo Builders

Bamboo Builders is a Singapore-based social enterprise that aims to #BuildChangeBetter. Believing every person should feel confident about their future, they close gaps in traditional education by empowering individuals with real-world skills to multiply real-world impact.

Since 2017, Bamboo Builders has trained tens of thousands of leaders in launching hundreds of initiatives that have made significant impact across Singapore and ASEAN. Their work spans across diverse communities, including youths, seniors, persons with disabilities, inmates, domestic workers and more. They have also worked with international foundations such as Google.org and ASEAN Foundation, governments, corporates and schools.

Find out more: bamboobuilders.org.

↗ About Google.org

Google.org applies Google's innovation, research, and resources to promote progress and expand opportunity for everyone.

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 report and no responsibility or liability whatsoever is accepted by any person of the Institute, its affiliates, and its respective officers, employees or agents.

Executive Summary

The rapid digital transformation of Southeast Asia (SEA) has unlocked economic opportunity but also created new vulnerabilities in the form of increasingly sophisticated scams and fraud. As millions of people and businesses come online, many are exposed to digital risk. Scams today exploit not only technical loopholes but also human trust, behavioural habits and systemic gaps, leading to erosion of trust, mounting financial losses and growing social harm across the region.

The dynamic threat landscape requires a shift from a narrow focus on cybersecurity to a broader, people-centred approach grounded in the principles of digital safety and resilience. Traditional security efforts have focused on protecting infrastructure from unauthorised cyberattacks. However, as scams increasingly rely on psychological manipulation and deception, SEA must adopt strategies that go beyond technical solutions to also strengthen societal and behavioural defences.

A resilience approach to anti-scam efforts spans the scam lifecycle. Proactive prevention, real time detection, victim support and long-term adaptation to evolving threats ensures interventions are not only reactive but also forward-looking and continuously improving.

The effort to build resilience requires a whole-of-society approach. Governments, businesses, civil society, community networks and end users all play critical roles in building digital resilience. By recognising the unique roles of each group, countries can foster inclusive, coordinated and sustainable responses that are appropriate and effective to each local context.

Concrete actions are already emerging across SEA that can be scaled, adapted, and replicated. Drawing from the experiences of the SEA-6 countries, the report outlines illustrative examples and practical recommendations under each resilience pillar, *Protect, Identify and Detect, Respond and Recover* and *Adapt*. These include expanding behavioural education campaigns, empowering trusted community voices, leveraging AI for detection, enhancing reporting pathways, strengthening cross-border law enforcement cooperation, improving victim care and updating outdated legal frameworks.

Finally, digital resilience is an ongoing endeavour. Beyond a whole-of-society approach and continued innovation, scam management efforts should be people-centred and culturally-aligned for the end-user. Moreover, as scams operate across borders, regional coordination and global cooperation are essential to tackling this cross-border threat.

1.
The Evolving Threat Landscape in Southeast Asia

The digital economy in Southeast Asia (SEA) has grown at an impressive pace, with a 27 percent compound annual growth rate since 2021.[1] By 2030, digitalisation is expected to contribute as much as US$1 trillion to SEA 's economy, fuelled by expanding internet access, mobile-first consumption habits, the rise of digital platforms and a vibrant startup ecosystem.[2] This growth offers opportunities for economic development, financial inclusion and cross-border trade.

Yet, this digital growth comes with corresponding risks. The speed of digital adoption has outpaced digital literacy, cybersecurity infrastructure and user awareness. Millions of individuals are coming online, many for the first time, without sufficient knowledge of how to navigate online risks safely. This gap has given rise to growing vulnerabilities, particularly among first-time internet users, small businesses and digitally-connected households. As the region embraces digital opportunity, the accelerating threat of cyber insecurity is one of the most pressing risks to the digital ecosystem both in the short and long term.[3]

1.1. From Security to Resilience: The Shifting Conversation

Businesses and governments have dealt with unauthorised cyber threats such as ransomware, data breaches, Distributed Denial of Service attacks and malware intrusions for over two decades. These attacks target systems and infrastructure, often breaching security without the victim's knowledge or consent. In 2023, the average cost of a data breach in SEA rose to US$3.05 million, and cyber extortion incidents increased by 42 percent across the region. Attacks on critical infrastructure are also a cause for concern, with a recent example being the targeting of Singapore's critical infrastructure by Advanced Persistent Threat (APT) actor UNC3886.[4]

While technical security threats continue to challenge organisational systems, individual users' day-to-day digital experiences are also increasingly at risk. Amongst the spectrum of online safety concerns, digitally-enabled scams and fraud have increased in frequency, complexity and impact. Unlike cyberattacks such as hacking and malware attacks may occur without the victim's knowledge or consent, scams and fraud schemes tend to rely on social engineering to convince individuals to share sensitive information or approve fraudulent transactions. Such "authorised" scams include investment fraud, romance scams, job scams and impersonation schemes. In Singapore, scam victims lost up to at least US$858 million in 2024, with self-effected transfers accounting for 82.4% of total reported scam cases.[5] In Vietnam, the Global Anti-Scam Alliance estimates that scam-related losses accounted for approximately 3.6 percent of national GDP in 2023.[6] The United Nations reported that cyber-enabled fraud caused losses of up to US$37 billion across East and SEA in 2023.[7]

The concept of digital resilience in the digital ecosystem is therefore broadening from the security of systems to keeping individual users safe.

1.2. Understanding Digitally-enabled Scams and Fraud

The terms scam and fraud are often used interchangeably across SEA. This is both in public discourse and institutional frameworks. In researching definitions across the region, there is no standalone legal definition of "scams". Rather they are usually prosecuted under the broader ambit of cheating or fraudulent activities. In Indonesia, for example, the overlap in terminology is largely due to the broad use of the word *penipuan*, which in Bahasa Indonesia refers to both "fraud" and "scam". This stems from the Indonesian Penal Code (KUHP), which offers a general definition of fraud as acts of deception intended to obtain something from another person through lies, trickery, or misrepresentation.[8] The Electronic Information and Transactions Law No. 11/2008 (UU ITE), as amended by Law No. 19/2016 and Law No. 1/2024, touches on fraud in digital contexts but does not provide a clear definition or categorisation.[9] Instead, it uses broad terms such as "misleading" or "false" information causing harm, which can apply to various situations beyond fraud alone.

A similar approach is seen in Singapore, where scams are prosecuted as "cheating" under the Penal Code 1871.[10] Fraud is likewise primarily defined and prosecuted under the Penal Code as cheating. The newly enacted Protection Against Scams Act, passed in 2025, reinforces this framework by placing scams under the same cheating provisions set out in the Penal Code.[11]

In the Philippines, there is also no legal definition of a scam. Instead, scamming is prosecuted under the offence of *Estafa* (swindling), as provided for in Articles 315 to 318 of the Revised Penal Code.[12] These same provisions are also applied in cases of fraud, reflecting the overlap in how the two terms are addressed in law.[13]

In Thailand, offences of cheating and fraud are addressed in Sections 341 to 344, 346, and 347 of Title XII "Offences against Property" in the Criminal Code, which are also used in both cases of scams.[14] In Malaysia, scams are not separately codified but fall under the broader category of cheating in Section 415 of the Penal Code.[15] Fraud is also prosecuted under this provision, with an additional offence of "fraudulent trading" targeting corporate misconduct under Section 540 of the Companies Act 2016.[16]

In Vietnam, fraud is addressed in Article 174 of the Penal Code 2015 (amended 2017) as the crime of "obtaining property by fraud."[17] Scams are not specifically defined in law but are prosecuted under the same provisions that govern deception and fraudulent activities.[18] Table 1 below covers the definitions of scams and fraud in SEA, with additional reference to relevant cybercrimes laws and related regulations.

Table 1: Definition of Scams and Fraud in SEA-6

Country	Definitions
Indonesia	• No standalone legal definition of scams; the term *penipuan* refers to both "fraud" and "scam" without distinguishing technical methods. • Fraud is defined in the Penal Code (KUHP) as deception intended to obtain something from another person through lies, trickery, or misrepresentation. • The Electronic Information and Transactions Law No. 11/2008 (UU ITE), amended by Laws No. 19/2016 and No. 1/2024, addresses fraud in digital contexts but does not provide a clear definition, instead using broad terms such as "misleading" or "false" information causing harm.
Singapore	• Scams are prosecuted as "cheating" under the Penal Code 1871. • Fraud is primarily defined and prosecuted under the Penal Code as cheating. • The Protection Against Scams Act (2025) reinforces this by placing scams under the same cheating provisions in the Penal Code.
The Philippines	• No legal definition of scams. • Scamming is prosecuted under *Estafa* or swindling in Articles 315–318 of the Revised Penal Code. • Fraud is prosecuted under the same laws, with no distinction between the two. • Additional charges possible under the Cybercrime Prevention Act (RA 10175), which expands criminal liability to acts committed through ICT means.
Thailand	• Scams and fraud are addressed under the same provisions: Sections 341–344, 346, and 347 of Title XII "Offences against Property" in the Criminal Code. • These cover cheating and fraud cases, including those involving digital means. • The Computer Crime Act (2017) specifically criminalises digital deception (e.g., online scams, data fraud and phishing).
Malaysia	• Scams are not separately codified, but they fall under "cheating" in Section 415 of the Penal Code. • Fraud is prosecuted under the same provision, with an additional offence of "fraudulent trading" targeting corporate misconduct under Section 540 of the Companies Act 2016. • Supplementary penalties may be levied under the Communications & Multimedia Act for digital infrastructure misuse.
Vietnam	• Scams are not separately defined but are prosecuted under the same provisions covering deception and fraudulent activities. • Fraud is defined in Article 174 of the Penal Code 2015 (amended 2017) as "obtaining property by fraud." • This is reinforced by the Law on Cyber Information Security and Decree 144/2021/ND-CP for cyber fraud penalties.

Source: Tech for Good Institute, 2025

For the purposes of this paper, we can broadly refer to the commonly accepted definitions of digitally-enabled scams and fraud in the literature. Fraud is a broad legal category encompassing any act of intentional deception for unlawful gain or to cause harm.[19] It often involves unauthorised or concealed actions, where the victim may remain unaware of the deception until after the harm has occurred. On the other hand, scams are a specific type of fraud that rely on direct psychological manipulation.[20] They use tactics such as fear, urgency, or emotional appeal to persuade individuals to willingly provide sensitive details, transfer funds or carry out actions against their own interest.

Both scams and fraud are rooted in deception and cause significant financial and emotional harm. While fraud typically involves manipulation of systems, scams target the individual, exploiting trust and behavioural triggers to achieve their aims.

As established in Table 1, digitally-enabled scams and fraud take on an additional dimension. While the base and foundational offence may fall under the penal code, violations can also be covered by cybercrime laws, computer misuse laws, and data protection and privacy laws. These legal frameworks are particularly relevant as they address the challenges posed by emerging technologies and the evolving nature of digitally-enabled scams and fraud.

The following types of scams are currently widespread across SEA.

↗ Phishing Scams

Phishing scams represent 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.[21]

Scammer employ sophisticated social engineering tactics, deliberately creating a false sense of urgency or fear to compel victims to act quickly without verifying the source. Common scenarios include claims of compromised accounts, overdue payments or suspended services, all designed to pressure victims into divulging confidential information.

The sophistication of modern phishing extends to meticulously-crafted spoofed websites and messages that closely mirror brands and communication styles of legitimate organisations. More targeted forms, such as spear phishing, utilise personal information to deceive specific individuals, with even greater precision.

The combination of accessible tools for creating convincing fraudulent communications and the widespread adoption of digital communication platforms makes phishing a persistent and rapidly evolving threat to both individuals and organisations.

↗ Case Study 1

WhatsApp Phishing Targeting Malaysian Digital Wallet Users[22]

In Malaysia, a sophisticated phishing campaign targeted GoPayz digital wallet users through WhatsApp. The scammers posed as official customer service representatives, contacting victims with urgent claims that their accounts required immediate attention due to security concerns or technical issues. Exploiting trust and authority, the perpetrators convinced victims to share their Transaction Authorisation Codes, claiming it was necessary to resolve problems.

This manipulation of trust resulted in substantial financial losses, with one victim losing up to USD20,700, an amount representing months or even years of personal savings for many individuals. This case exemplifies how phishing scams exploit both trusted communication platforms and the human tendency to comply with apparent authority figures during moments of perceived crisis. It underscores the critical importance of user education and the need for service providers to implement robust security measures and comprehensive fraud awareness programmes.

↗ Impersonation of Authority Scams

Impersonation scams involve malicious actors posing as trusted authority figures, such as government officials, police officers or corporate representatives to manipulate victims into complying with fraudulent requests.[23] These schemes exploit fundamental human psychology, particularly our ingrained respect for authority and tendency to comply with official directives. Perpetrators typically construct elaborate scenarios designed to invoke fear, urgency or concern about legal consequences. Common narratives include claims of unpaid fines, involvement in criminal investigations or urgent administrative issues immediate attention.

To enhance their credibility, scammers employ various sophisticated techniques, including official-sounding language, forged documentation and spoofed telephone numbers that mimic legitimate institutions. This tactic also involves convincing victims to install malicious software disguised as legitimate government or corporate applications, granting scammers full access to personal and financial data.

These scams are especially effective, as victims' desire to comply with authority or resolve perceived threats often overrides their natural caution.[24] The use of real-time communication, particularly telephone calls, adds pressure and reduces victims' ability to pause and verify the interaction's legitimacy.

↗ Case Study 2

Vietnamese Government Officer Impersonation[25]

In Hanoi, a 43-year-old woman lost VND 3 billion (approximately US$110,000) to an impersonation scam. Posing as a police officer, the scammer contacted the victim to install a specialised application for identity card processing, an administrative task that appeared routine and harmless.

The scammer's approach was highly sophisticated, exploiting the victim's trust in authority whilst referencing a common bureaucratic process. Once the fake app was installed, it granted the scammers full access to her banking information, enabling them to drain her accounts.

This case highlights how impersonation scams exploit both trust in official institutions and the familiarity of routine administrative procedures. It emphasises the critical importance of verifying unsolicited requests through official channels and avoiding the installation of unverified software, regardless of how the request may appear.

Romance Scams

Romance scams target individuals seeking emotional or romantic connections, exploiting the human desire for companionship and affection. These schemes often begin on online platforms, including dating applications and social media networks, where scammers can easily create elaborate false identities.[26] They typically pose as attractive, successful professionals such as doctors, engineers or military personnel, using these fabricated identities to gain trust and admiration while offering plausible reasons for limited communication or an inability to meet in person.

The relationship develops gradually, with scammers investing weeks or months to build emotional intimacy through consistent communication, flatter and fabricated life histories. Once sufficient trust is established, the scammer introduces a sudden crisis, such as a medical emergencies, travel difficulty or legal problem, requesting immediate financial assistance.

These schemes often involve sophisticated supporting evidence, including fake documents, stolen photographs, and elaborate backstories to support their claims. Romance scams can be particularly devastating because they exploit emotional vulnerabilities, often targeting individuals who may be lonely, isolated or particularly trusting.

Case Study 3

Executive Defrauded in Thai Romance Scam[27]

A 50-year-old chief financial officer at a manufacturing firm in Thailand became the victim of an extraordinarily sophisticated romance scam that ultimately resulted in her imprisonment. The scammer created a convincing LinkedIn profile, purporting to be a US army doctor, complete with professional credentials and military background. Over six months, the scammer manipulated emotions and forged documents to gain the victim's trust, while escalating financial requests.

The financial impact was catastrophic, with the victim transferring 6.2 billion baht (approximately US$190 million) from company accounts. The scheme was later linked to a Nigerian fraud network highlighting the international reach of romance scams. Following the discovery, the victim was arrested and sentenced to a 20-year prison, underscoring the severe legal consequences that can result from falling victim to such schemes. This case illustrates the devastating toll romance scams can take, not only financially, but also on professional reputation and personal freedom. It highlights the critical importance of individuals maintaining healthy scepticism in online relationships, while organisations must implement rigorous internal controls for large financial transactions.

↗ Fake Friend Scams

Fake friend scams exploit the trust built into personal relationships by utilising compromised or fabricated social media accounts that mimic those of victims' friends, family members or acquaintances. Because the messages appear to come from known contacts, they lower the victims' natural scepticism[28] and increase the likelihood of compliance.

Fraudsters typically hijack existing accounts or create new ones using stolen photos and personal information. This enables them to craft convincing narratives, often referencing mutual friends or shared experiences, to make their requests appear credible. Common scenarios involve urgent pleas for help with medical bills, travel expenses or legal fees, delivered via real-time messaging platforms that heighten the sense of urgency.

The emotional weight of these scams makes them especially difficult to resist. Victims are driven by concerns for a genuine friend or family member, making them more likely to respond to offer assistance without verifying the situation. This emotional manipulation, combined with the apparent authenticity of the communication source, makes fake friend scams remarkably effective.

↗ Case Study 4

Indonesian University Student Targeted by Friendship Fraud[29]

An Indonesian university student reported a sophisticated fake friend scam involving compromised Facebook accounts belonging to her genuine friends. The fraudsters requested money for fabricated emergencies, including a nephew's urgent surgery that supposedly required immediate payment. The scammers maintained consistent communication and even demanded proof of payment, adding to the deception's realism.

The student became suspicious due to subtle inconsistencies in communication style and unusual requests for financial assistance. Demonstrating notable initiative, the student engaged with the scammer for three hours, successfully tracing their IP address and gathering evidence for a police report. This case highlights how fake friend scams exploit trusted relationships. It also underscores the critical importance of cross-checking unusual messages directly with the friend through alternative channels.

↗ Employment Scams

Employment scams target vulnerable individuals with false promises of lucrative employment opportunities, often requiring upfront payments for processing fees, training costs or travel documentation.[30] These schemes frequently serve as fronts for human trafficking networks, exploiting desperation for better economic opportunities.

Fraudsters advertise positions through social media platforms and legitimate job boards, offering attractive salaries for roles in call centres, hospitality or other service industries, often in foreign countries. The international aspect of these opportunities is used to explain requirements for upfront payments and complex travel arrangements.

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.

The cross-border nature of these scams, involving complex travel routes and fraudulent documentation, makes them particularly difficult to trace and prosecute. Employment scams prey upon economic vulnerabilities and trust in seemingly legitimate recruitment processes, often targeting individuals facing financial hardship or limited local opportunities.

↗ Case Study 5

Philippine Human Trafficking Network Exposed[31]

The Philippine Bureau of Immigration uncovered a sophisticated human trafficking network that recruited victims through social media platforms using fraudulent job offers for call centre positions in Laos. The scheme targeted individuals seeking better economic opportunities abroad, exploiting their trust in seemingly legitimate recruitment processes. Two victims, intercepted at Clark International Airport, each paid up to US$700 for fraudulent travel documents and processing fees.

The investigation revealed a complex travel route through Thailand and connections to broader criminal operations, including cryptocurrency fraud and illicit nightclub employment. This case demonstrates the transnational nature of employment scams and their links to human trafficking and financial exploitation. The swift intervention by immigration authorities highlights the crucial role of border security in detecting and preventing such schemes, whilst the substantial upfront payments demanded illustrate the financial vulnerability of victims. It highlights the the value of having job seekers verify overseas employment offers through official government channels. For governments, it is also important to strengthen international cooperation, ensuring more effective disruption to cross-border trafficking networks.

With the advent of new technologies, scams and other fraudulent activities are becoming increasingly sophisticated in how they reach wider society. The growing accessibility of Artificial Intelligence (AI) has introduced new forms of scams, making those already discussed even harder to detect. Deepfakes, for instance, can intensify phishing schemes, impersonation of authorities, romance scams, fake friend scams and employment scams.

🡕 Deepfake Scams

Deepfake scams use AI to create highly realistic yet entirely fabricated audio or video content. It can be used in conjunction with other schemes, such as impersonation scams, but typically exploit the recognition, legitimacy and public trust of public figures or trusted individuals, from politician to celebrities and business leaders to family members.[32]

The technology behind deepfakes manipulates facial expressions, lip movements and voice patterns with remarkable precision, to produce content that appears authentic to the untrained eye. The growing accessibility of deepfake tools has lowered the barrier to entry for cybercriminals.[33] Alarmingly, it requires minimal input such as a few images or seconds of audio to generate convincing fake content.

These videos are often enhanced with familiar logos, media branding and professional quality production to reinforce the illusion of authenticity and trustworthiness. By leveraging our instinct to believe what we see and hear, deepfake scams can bypass the scepticism that might arise with text-based fraud.

🡕 Case Study 6

Singapore Deputy Prime Minister Deepfake Investment Scam[34]

A deepfake scam on Facebook and Instagram in 2024 featured a deepfake of Singapore's then-Deputy Prime Minister Lawrence Wong endorsing a dubious investment scheme. The video demonstrated sophisticated manipulation techniques, utilising real interview footage with fake audio that mimicked Wong's distinctive speaking style and intonation.

To make the scam look more credible, the fraudster added The Straits Times' logo and branding, creating the false impression that the video was supported by legitimate news outlets. This misuse of trusted media branding represents a concerning evolution in scam tactics.

Deputy Prime Minister Wong publicly denounced the scam, while experts like Associate Professor Terence Sim warned about how easy it is becoming to create deepfakes. This incident clearly shows how AI-powered scams can exploit public trust. For individuals, it is important to highlight the need to verify online media content. In addition, clearer labelling of AI-generated content would help users distinguish between authentic and manipulated material.

These examples of digitally-enabled scams and fraud highlights an important shift that "what is secure does not necessarily mean safe". Even the strongest cybersecurity systems can be circumvented by threats that prey on trust, fear and urgency. As threats increasingly target individuals, building resilience means not only defending against breaches but also empowering users to withstand manipulation, recover from harm and adapt to future threats.

1.3. Navigating an Increasingly Complex Scams Landscape

The range and creativity of scam types capitalise on underlying systemic challenges in the SEA digital landscape. Common challenges extend beyond individual user behaviour and digital literacy to enforcement capacity, legal frameworks and cross-border coordination. This section explores common areas for improvements to strengthen resilience against digitally-enabled scams.

Figure 1: Key Challenges in Southeast Asia's Scams and Fraud Landscape

Challenges in
Southeast Asia's Scams
and Fraud Landscape

Sophistication of Scams and Fraud

Gaps in Public Awareness & Literacy

Fragmented Ecosystem Efforts

Outdated Legal Frameworks & Limitations
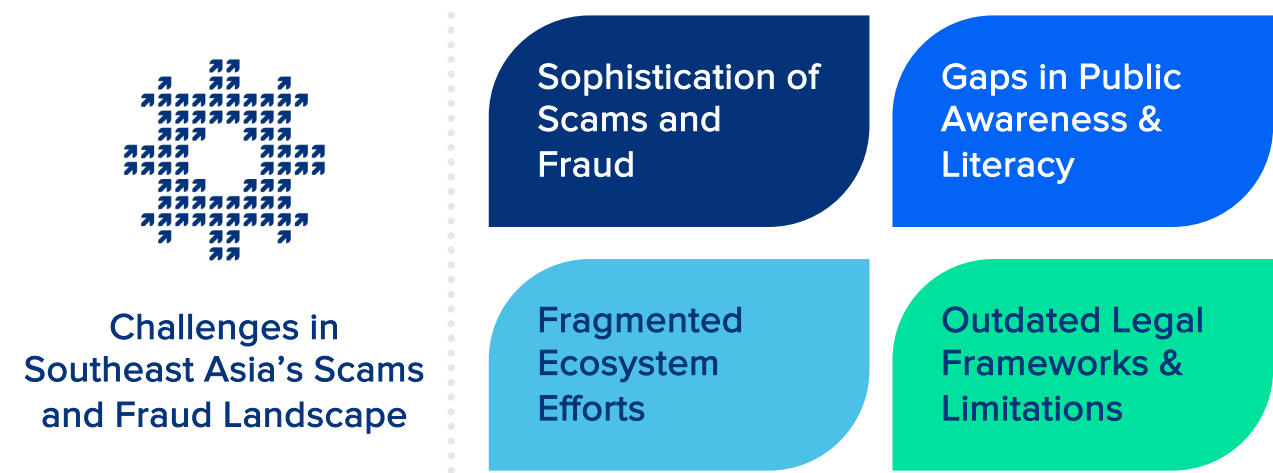
Source: Tech for Good Institute, 2025

Increased sophistication of scams and fraud tactics

Scams in SEA continue to evolve in both scale and sophistication. Surprisingly, however, the offline nature is still very prevalent. In the Philippines, for example, we heard cases of "shoulder surfing" in local shops, where scammers discreetly observe victims entering mobile wallet PINs during over-the-counter top-ups, then steal funds.[35] These low-tech tactics continue to be surprisingly effective. Scammers also exploit communication channels, using local phone numbers for scam calls and SMS to make their schemes appear more credible.

On the digital front, this sophistication has been fuelled by the increasing adoption of advanced technologies such as AI, deepfakes and refined social engineering tactics. According to a January 2024 report by the United Nations Office on Drugs and Crime (UNODC), deepfakes are now being used to "execute social engineering scams with alarming success rates, exploiting people's trust and emotions."[36] From 2022 to 2023 alone, the Asia-Pacific region saw a staggering 1,530 percent increase in deepfake-related fraud.[37] In response, countries such as Malaysia, Singapore and Indonesia have issued public warnings to raise awareness of this growing threat.[38]

Finally, scammers are increasingly turning to cryptocurrencies. Victims are pressured to transfer funds into crypto wallets, bypassing banking safeguards. Given the anonymity of many crypto transactions, this makes recovery and enforcement extremely difficult.

Gaps in digital literacy and response awareness

The growing sophistication of scam tactics is further complicated by widespread gaps in digital literacy and scam awareness. First-time internet users, especially in rural areas, among the elderly, the youth and underbanked communities, often lack the foundational knowledge needed to recognise and respond to digital threats. The vulnerability of these groups is exacerbated by the rapid expansion of digital services and the slower rollout of effective digital awareness and education programmes, leaving many users unprepared and unprotected.

In addition to the lack of preventive awareness, many individuals are also unaware of how to respond appropriately when scams occur. A significant number of victims do not report incidents, often due to a lack of trust in law enforcement or a belief that reporting will not result in meaningful action. For example, 67 percent of scam victims in Thailand did not report their scams after they had experienced it.[39] In Singapore, two in three citizens say they would not know how to respond to a scam.[40] A recent report, produced by the Tech for Good Institute for Bamboo Builders, also notes that many rely on family and friends as primary sources of information about scams, often surpassing government agencies or financial institutions. While community trust is important, misinformation and informal advice can delay or prevent timely action, allowing scammers to escalate further. This combination of underreporting and informal knowledge-sharing reflects a deeper gap in public education and institutional outreach that must be addressed.[41]

Fragmented and siloed ecosystem efforts

Across SEA, efforts to combat scams often remain fragmented at the national level, with multiple agencies often operating in parallel. Police forces, telecommunications regulators, banks, digital platforms, and financial authorities each oversee different aspects of scam response.[42] This frequently results in overlapping mandates, unclear referral processes and inconsistent support for victims. The lack of integration creates critical gaps in threat intelligence, delays enforcement efforts and leads to public confusion. Without streamlined national systems, victims are often uncertain about which response plan to follow or where to seek help.

These domestic challenges are further compounded by the absence of effective cross-border collaboration. Many scams are transnational, involving perpetrators in one country, targeting victims in another, and digital infrastructure hosted elsewhere.[43] Yet national law enforcement agencies often lack the legal authority or operational capacity to act beyond their jurisdictions. Legal inconsistencies, limited diplomatic coordination and the absence of shared protocols may slow down joint investigations.[44] In addition, countries across the region lack shared databases and real-time alert systems or harmonised legal frameworks, making it difficult to track criminal actors or financial flows across borders.

Outdated legal frameworks and regulatory limitations

Legal frameworks in many SEA jurisdictions require significant updates to remain fit-for-purpose in today's rapidly evolving threat landscape. Existing legislation must be adapted to address emerging forms of crime, including AI-enabled scams, deepfake impersonation, and cryptocurrency-based money laundering. In Malaysia, for example, while laws such as the Computer Crimes Act 1997 and the Personal Data Protection Act 2010 provide a foundational basis for cybersecurity enforcement, there is room for refining provisions so that it specifically addresses sophisticated online fraud and transnational cybercrime networks.[45]

Participants also pointed to the need to review and modernise other legal instruments. In the Philippines, the SIM card registration law was highlighted as needing stronger controls to prevent misuse in scam operations.[46] There is also a growing need to update laws governing human trafficking and business registration, which are increasingly exploited by scam syndicates to support fraudulent schemes. Without responsive and timely legal frameworks, enforcement agencies are left with limited tools to deter, investigate and prosecute offenders effectively.

Addressing these complex threats requires a broader collective effort. Tackling scams effectively demands the involvement of a wide range of actors—not just governments and enforcement agencies, but also businesses, civil society, communities and individuals. The next step is to understand how these actors can play meaningful roles and work together to build a safer and more resilient digital environment.

2.
Operationalising a Whole-of-Society Approach to Build Resilience

Recognising the complex and rapidly evolving nature of scams and fraud in SEA, the Tech for Good Institute proposes a *whole-of-society* approach as a guiding framework for action. But what does this actually mean in practice, particularly within the regions' diverse social, institutional, and digital landscapes?
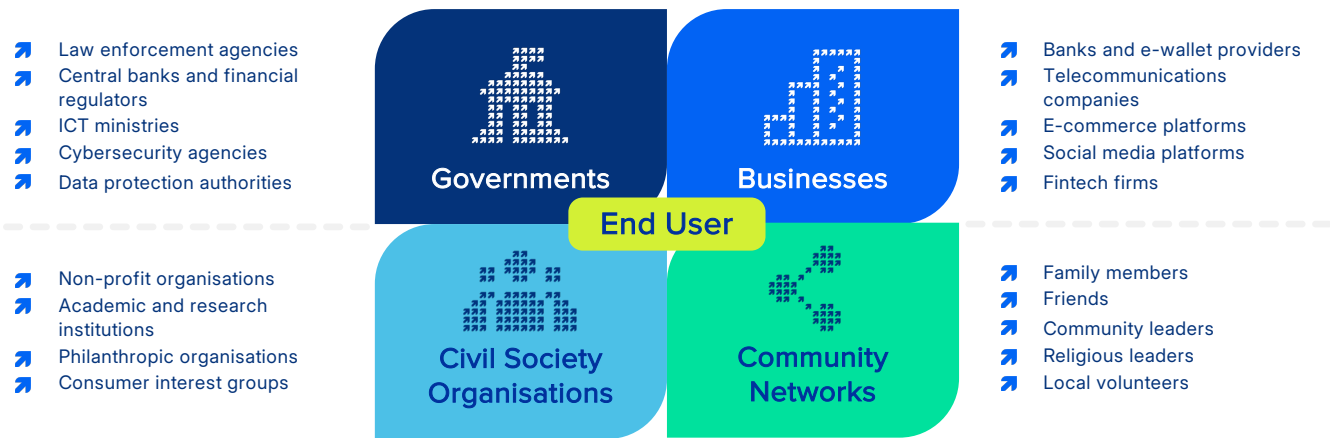
A whole-of-society approach is based on the principle that no single entity can effectively tackle scams and fraud alone. Drawing from the definition put forward by the United Nations Educational, Scientific and Cultural Organisation (UNESCO), it calls for collective efforts of public authorities, the private sector, and civil society to pursue shared policy goals.[47] A key element of this approach is the integration of both formal and informal institutions, recognising that sustainable governance depends on inclusive, multi-stakeholder collaboration.[48] Crucially, it reframes the idea of "governance" as more than just government, emphasising the need for cooperative engagement across all sectors of society.

In the context of SEA, roundtable participants emphasised the critical role of community in building digital resilience. Beyond the efforts of government agencies, private sector entities, and civil society groups, the contributions of *community networks* and grassroot actors must not be overlooked. Across the region, family members, neighbours, religious leaders and local influencers often serve as trusted sources of information and support. Their influence in raising awareness, shaping behaviour and reinforcing social norms plays a vital role in addressing scam risks at the grassroots level.

This focus on community aligns closely with UNESCO's definition of a whole-of-society approach, which highlights the inclusion of *informal* institutions and stakeholders in governance frameworks. Recognising their importance ensures that responses to scams and fraud are not only effective but also culturally and socially grounded.

This chapter outlines the distinct roles and contributions each stakeholder group can make in strengthening cyber resilience across SEA.

Figure 2: A Whole-of-Society Approach to Building Digital Resilience

- Law enforcement agencies
- Central banks and financial regulators
- ICT ministries
- Cybersecurity agencies
- Data protection authorities

Governments

Businesses

- Banks and e-wallet providers
- Telecommunications companies
- E-commerce platforms
- Social media platforms
- Fintech firms

End User

- Non-profit organisations
- Academic and research institutions
- Philanthropic organisations
- Consumer interest groups

Civil Society Organisations

Community Networks

- Family members
- Friends
- Community leaders
- Religious leaders
- Local volunteers

Source: Tech for Good Institute, 2025

2.1. Government: Setting the Policy and Enforcement Foundation

Government institutions and regulatory bodies are central to national digital resilience. Their responsibilities span legislation, law enforcement, inter-agency coordination, and international collaboration. One of their most critical roles is the development of robust legal frameworks that can keep pace with emerging threats.[49] For example, Thailand has introduced legislation that holds banks and telecommunications companies accountable for failures in scam prevention, signalling a shift towards institutional responsibility.[50] In Singapore, the recently released Shared Responsibility Framework outlines the allocation of liability for losses resulting from specific types of phishing scams, along with the operational workflow for consumers to report such incidents.[51] Meanwhile, the Philippines has enacted the Anti-Financial Account Scamming Act (AFASA), which establishes a coordination mechanism between the central bank and law enforcement agencies to respond more effectively to financial scams.[52]

Beyond legislation, governments need to ensure that victims have access to clear, responsive and accessible escalation channels. National hotlines and digital reporting platforms serve as critical lifelines for individuals seeking timely support and redress.[53] These systems not only assist victims but also generate vital data to inform prevention strategies and policy responses.[54]

Finally, governments have a pivotal role in leading and enabling cross-border collaboration. Transnational scams require coordinated responses that go beyond national jurisdictions. Effective cooperation through intelligence sharing, extradition agreements and joint investigations is vital to dismantling international scam networks and closing enforcement gaps across the region.

2.2. Businesses: Enabling a Safe User Experience

The private sector, particularly financial institutions, telecommunications companies, and digital platforms, plays a critical role in safeguarding the digital ecosystem. Their responsibilities include securing their systems, leveraging their extensive reach to raise public awareness and supporting vulnerable groups. Ensuring compliance with industry standards is a key aspect of maintaining trust and integrity in their platforms. Companies are incentivised to do so not only to meet regulatory requirements, but also to preserve user confidence and sustain engagement in an increasingly digital environment. Closer coordination with governments can also lead to more timely and aligned responses, especially when combating fast-evolving scams that cut across sectors.

Given their position at the forefront of technology and innovation, businesses can deploy advanced tools to build digital resilience. This includes AI for real-time scam detection, biometric authentication, scam screening systems, and fraud detection algorithms. These interventions help mitigate risks before they escalate.[55] Furthermore, businesses can lead in promoting safe digital behaviours by embedding user education into their platforms and outreach campaigns.[56] By sharing resources, expertise, and practical toolkits, especially with smaller enterprises, the private sector can help raise the baseline of digital safety across the broader economy. In doing so, they contribute to a more resilient, secure and inclusive digital landscape.

2.3. Civil Society: Catalyst for Education, Research, and Advocacy

Civil society serves as a key pillar in the whole-of-society response to scams and fraud, offering essential expertise, outreach, and advocacy that complement the roles of governments and businesses. Civil society actors, including NGOs, advocacy organisations, academic institutions and training centres, play a critical role in shaping awareness, informing policy and building long-term capacity to prevent scams. These groups act as vital intermediaries between the public, private sector and government, ensuring that diverse perspectives, particularly those of vulnerable or marginalised communities, are reflected in scam prevention strategies.

Each segment of civil society plays an important role. NGOs can lead targeted outreach and victim support, particularly for vulnerable groups such as migrant workers, the elderly, and low-income communities. Academic institutions contribute evidence-based research and curriculum development, helping to shape public discourse and inform both policy and practice. In some countries, partnerships between civil society organisations and education providers have led to the rollout of digital safety training at the community level, equipping citizens with foundational knowledge to recognise and avoid scams.[57] There is growing recognition of the importance of investing in civil society-led training and public education infrastructure, including certified programmes for digital literacy and consumer protection. Supporting the formalisation and scale-up of these efforts can ensure sustained, community-driven impact across sectors and populations.

2.4. Community Networks: Informal Linkages and Everyday Influencers

While formal institutions are critical to combating scams and fraud, roundtable participants consistently emphasised the important role of informal community networks. These include family members, neighbours, friends, religious leaders and other trusted figures embedded in daily life. In rural or low-connectivity areas, these actors are often the first point of contact when someone encounters a scam. Across SEA where trust and relationships are central, people frequently rely on word-of-mouth advice over formal channels. For instance, in Singapore, many individuals turn to family and friends for scam-related information.[58] With this, participants shared that there is also significant potential to involve community and religious leaders in scam awareness initiatives by incorporating safety messages into sermons, community events and local gatherings.

While these informal networks are powerful channels for spreading awareness, they can also perpetuate misinformation or outdated advice. Strengthening this "digital community" involves equipping everyday influencers with accurate, accessible and culturally relevant resources so they can serve as credible messengers in their communities. Public awareness campaigns that recognise and empower these informal actors as partners in digital safety can enhance both reach and trust. By integrating informal networks into broader digital resilience strategies, societies can better protect individuals at the grassroots level. These efforts can be a vital complement to institutional responses, helping to close gaps in education, outreach and real-time scam prevention.

2.5. End Users: Making Informed Decisions

End-users, including individuals, consumers, and the general public, are a critical part of defence against scams and fraud. Their awareness, vigilance, and reporting behaviour directly shape the effectiveness of broader ecosystem responses. It is therefore vital to equip users with accurate, accessible information that enables them to make safe decisions online.

However, a persistent confidence-skills gap must be addressed. For example, while 84 percent of Singaporeans report feeling confident in identifying scams, fewer than half are able to accurately detect phishing attempts.[59] This overestimation can lead to a false sense of security and increased vulnerability to attacks.

Improving behavioural resilience is essential. Awareness efforts must move beyond one-off warnings toward the development of sustained, risk-aware digital habits. End users must take an active role and responsibility for their own online safety, remaining alert to red flags and informed about evolving scam tactics. Regardless of how strong institutional safeguards may be, a scam can still succeed if a user authorises a fraudulent transaction. In one roundtable discussion, participants compared this dynamic to road safety, where governments may build and enforce a secure infrastructure, but the individual driver still bears responsibility for staying alert and making safe choices behind the wheel.[60] Similarly, a resilient digital environment requires both system-level protections and empowered, informed users.

In operationalising a whole-of-society approach, it is equally important to apply key cross-cutting principles that ensure initiatives are both effective and inclusive. Roundtable participants across the region emphasised that efforts to build resilience against scams and fraud must be:

- **Cross-Disciplinary:** integrate technical, behavioural, policy and design expertise to create holistic and innovative solutions that address scams from multiple angles.

- **Cross-Sectoral:** promote active coordination across government, industry, civil society and media, ensuring all sectors share responsibility in building digital resilience and more coherent responses to emerging threats.

- **Cross-Cultural:** localised to reflect the diverse languages, cultural values and digital behaviours present across SEA, making interventions more relevant, trusted and effective.

- **Cross-Border:** strengthen regional and international cooperation through joint mechanisms and partnerships to combat cross-jurisdictional and transnational scam threats.

These principles are critical for embedding resilience across all parts of society and provide a foundation for the more targeted, phase-specific interventions outlined in the next chapter.

3.
Digital Resilience Throughout the Scam Lifecycle

To effectively counter scams and fraud, it is essential to understand not only *who* should be involved but also *when* interventions should take place. This chapter highlights the need to build digital resilience across the entire scam lifecycle. By breaking down the journey of a scam into distinct stages, this helps stakeholders identify key opportunities for prevention, detection, response and adaptation. It offers a practical tool for governments, businesses, civil society and communities to coordinate their efforts more effectively, ensuring that interventions are timely, targeted and responsive to evolving scam tactics.

3.1. Understanding the Scam Life Cycle

Scams and fraud do not occur in a single moment. They unfold over time and multiple stages, each involving a series of calculated steps carried out by perpetrators. For example, financial crime platform FeedzAI outlines three technical phases of cyber-enabled fraud: *customer access*, *transaction* and *monetisation*.[61] Another model breaks down the anatomy of a scam into "3 Cs": *connection, convincing and conversion*.[62] The United Nations Development Programme (UNDP) also presents a more detailed framework in its *Anti-Scam Handbook*, highlighting the layered complexity of scam where the steps are largely categorised into: *pre-scam, during a scam* and *post-scam*.[63]

Across various frameworks that map the scam lifecycle, a common structure emerges: scams can be broadly categorised into three key stages of: before, during and after the scam. This structure is well-supported in existing literature,[64] and this report does not seek to reinvent the wheel. Rather, it builds on this established conceptualisation by streamlining the victim journey into these three critical phases.

One key addition from this report is the concept of resilience and adaptation as a guiding concept. This adaptive mindset is particularly relevant for SEA. The goal is not only to survive a scam incident but to emerge stronger from it. Ideally, when a similar scam reoccurs, individuals and systems will recognise warning signs earlier or better yet, have new safeguards in place to prevent the threat from taking hold. This continuous cycle of learning and adaptation strengthens digital resilience. It ensures the broader ecosystem stays ahead of malicious actors and becomes more capable of anticipating, mitigating and recovering from the future threats.

3.2. Targeted Approach for Digital Resilience

Building on the Tech for Good Institute's Cyber Resilience Framework, there is an opportunity to provide a structured approach for identifying targeted responses across the entire scam and fraud lifecycle.[65] It outlines four key pillars of intervention: *protect, identify and detect, respond and recover* and *adapt.* As highlighted earlier, resilience in this context refers not merely to the capacity to respond and recover, but also the ability to *adapt–to* anticipate future threats and evolve in response. Building this resilience therefore, requires ongoing learning and preparation, not just reactive measures.

Understanding the stages of a scam–before, during, and after–constitutes only a foundational step. But true resilience depends on the systematic integration of well-timed, coordinated actions throughout the entire lifecycle. Each phase presents distinct opportunities for prevention, mitigation and recovery. A strategic, multi-stakeholder approach is essential to ensure that responses are not only effective but also timely and adaptive.

What does this look like in practice?

Figure 3: Targeted Interventions throughout the Scam Victim Journey
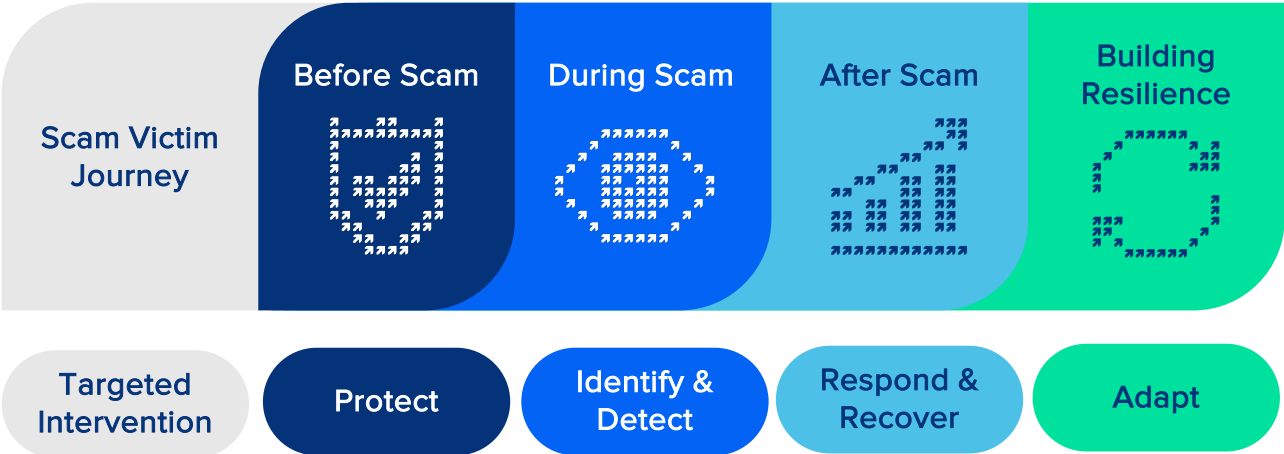
Source: Tech for Good Institute, 2025

↗ **Protect:** What can be done before a scam occurs? This includes measures such as public awareness campaigns, digital literacy training, behavior-change initiative and pre-emptive platform safeguards.

↗ **Identify and Detect:** What helps individuals recognise and avoid scams in real time? This might include scam alerts, real-time warnings, user verification tools, anomaly detection systems and notification mechanisms.

↗ **Respond and Recover:** How do we support victims after an incident? This involves clear reporting mechanisms, access to support services and hotlines, and where feasible, financial restitution.

↗ **Adapt:** How do we future-proof our systems, policies, and behaviours to stay ahead of constantly evolving scam tactics? This pillar includes systemic learning, regular updates to regulation and enforcement protocols, and the proactive redesign of platforms based on new patterns of fraud.

It is important to recognise, however, that these interventions do not occur in strict sequence, nor do they operate in isolation. While the approach is structured into four pillars, the actions under each pillar can overlap and reinforce one another. It should also be pursued simultaneously. Crucially, adaptation does not require prior victimisation. Systems and individuals can proactively adapt in anticipation of future threats. By pursuing protection, detection, response and adaptation in parallel, society can strengthen their overall digital resilience and reduce risks across the entire scam lifecycle.

3.3. Bridging Ideas to Action: Of a Whole-of-Society Approach and Resilience

The four pillars noted in this chapter provide a structured way to address scams and fraud across the entire lifecycle, but their effectiveness depends on collective action from across society. Each pillar of *Protect, Identify and Detect, Respond and Recover* and *Adapt* presents unique opportunities for governments, businesses, civil society, community networks and end users to contribute in complementary roles. Resilience is not built through isolated interventions but through coordinated and sustained action, combining institutional leadership, grassroots action and empowered individuals.

Turning ideas into action requires grounding them in the social, cultural, and institutional realities of SEA. This means tailoring strategies to the region's unique contexts while ensuring inclusive participation and shared accountability.

Chapter 4 builds on this foundation by offering concrete, actionable recommendations for each pillar. These recommendations draw from regional experiences and are designed to be adaptable to local contexts. It also showcases real-world examples of whole-of-society collaboration, demonstrating the power of cross-sector partnership in strengthening digital resilience across SEA.

4. Building Digital Resilience in Southeast Asia

As digital adoption accelerates across all sectors of society, efforts to protect users, detect threats, respond swiftly, and continuously adapt to emerging risks must evolve in tandem. This chapter focuses on *how* to build digital resilience by presenting concrete, actionable recommendations for building digital resilience across SEA. Drawing from country-specific insights and roundtable discussions, it highlights practical interventions that can be scaled, adapted and shared across different national and community contexts.

These recommendations are grounded in two key ideas introduced earlier in the report: the Whole-of-Society Approach (Chapter 2) and the Digital Resilience (Chapter 3). The Whole-of-Society Approach recognises that governments alone cannot build resilience. Instead, digital safety must be co-created by an ecosystem of actors, including businesses, civil society, community networks and end users. The concept of Digital Resilience meanwhile, structures anti-scam and fraud efforts across four interconnected pillars: *Protect, Identify and Detect, Respond and Recover* and *Adapt.*

At every stage of the resilience journey, different stakeholders are uniquely positioned to lead, support or scale action. For example, governments can establish legal guardrails and national response infrastructure, while businesses can embed safety features and educate their users. In addition, civil society organisations can drive outreach, advocacy and education. Community leaders can localise interventions and build trust at the grassroots. End-users, in turn, can become active participants by adopting protective habits in their daily lives and remaining alert to evolving threats.

By combining a whole-of-society mindset with a targeted, phase-specific approach, SEA can foster a resilient digital ecosystem, one that protects users, sustains public trust, and ensures no one is left behind. The recommendations that follow are supported by specific examples and selected case studies from across the region. This chapter, while not exhaustive, is intended to spark further innovation, inform future policymaking and promote cross-border collaboration.

4.1. Protect: Proactive Measures

The *Protect* pillar focuses on reducing the risk of scams through proactive, preventive measures. This includes not only technical safeguards, but also public education, behaviour-change initiatives and trusted community engagement. It serves as the foundation for building long-term digital safety.

Prevention is often recognised as one of the most effective and scalable approaches to addressing digital threats. While response and recovery are vital, they typically occur after harm has already taken place. This may involve financial loss, reputational damage or psychological distress. Protection, in contrast, is about reducing vulnerabilities before harm occurs, by improving user awareness and promoting safe digital habits from the outset.

Drawing on insights from the regional roundtable discussions, the table below outlines how different stakeholder groups can contribute to the *Protect* pillar.

Table 2. Protect: A Whole-of-Society Approach

Stakeholder Group	Potential Roles and Responsibilities in Protection
Government	• Integrate digital safety into national education curricula and public campaigns • Fund behaviour-change initiatives and inclusive digital literacy programmes • Support the formal involvement of community educators and trusted messengers on the ground • Establish regulatory incentives and minimum standards for scam prevention in businesses • Promote MSME resilience through procurement policies and targeted grants
Businesses	• Embed scam prevention tools and educational prompts into digital platforms (e.g. banking apps and telecom services) • Collaborate with government and civil society on awareness campaigns and user engagement • Offer low-cost, user-friendly digital safety solutions tailored for MSMEs • Build trust by reinforcing customer protections and support after scam incidents have occurred • Amplify trusted voices through branded content and community outreach

Stakeholder Group	Potential Roles and Responsibilities in Protection
Civil Society Organisations	• Design and deliver inclusive digital literacy training, especially for vulnerable or marginalised groups • Develop culturally and linguistically appropriate awareness materials • Mobilise and mentor local trusted messengers (e.g. volunteers, religious figure and community leaders) • Support MSMEs and informal workers with scam preparedness resources • Reduce stigma through community-based education and advocacy
Community Networks	• Disseminate scam awareness messages through trusted social/local structures (e.g. churches, temples and local councils) • Train and activate intergenerational educators (e.g. youth teaching elders) • Host local events and forums to discuss scam prevention and share experiences between community members • Act as peer support groups or first responders in the event of a scam • Reinforce safe digital behaviours through repeated community engagement
End Users	• Adopt safe digital habits (e.g. verifying links, avoiding suspicious apps) • Participate in literacy campaigns and peer learning • Report scams and share protective knowledge with family, friends and co-workers alike • Help older or less digitally literate individuals to identify and avoid scams • Apply scam prevention practices in daily life and business operations

Source: Tech for Good Institute, 2025

The roles outlined above set the foundation for collective action under the *Protect* pillar. The roundtable participants also surfaced real-world examples across the SEA-6 countries, showcasing initiatives and potential models that illustrate how protective measures can be adapted to local contexts, scaled through collaboration, and reinforced across digital, institutional and community environments alike.

⬈ Run Digital Literacy and Behaviour-Change Education Campaigns

Across SEA, digital literacy is often equated with general awareness. However, knowledge alone does not always translate into safer behaviours. People may recognise that scams exist, yet still fall victim due to overconfidence, routine digital habits, or limited exposure to real-world scam tactics. In Malaysia, an estimated 70 percent of scam victims never report their cases, pointing to not only fear or stigma but also a broader lack of preparedness and accessible support.[66]

To build meaningful protection, digital literacy efforts must evolve into behaviour-change campaigns that are ongoing, practical and context-sensitive. Roundtable participants underscored the importance of using digital platforms as a key delivery channel. In Vietnam, where over 72 million people are active on social media, platforms such as Zalo, TikTok and Facebook were identified as critical for reaching both youth and rural communities.[67] Participants also recommended collaborating with influencers and content creators to deliver messages in engaging formats—such as meme-based videos, live Q&As, gamified conten, and relatable short clips. These formats were seen as especially effective for younger audiences or those with limited formal digital education, making them highly accessible.

Campaigns must go beyond raising awareness to changing behaviours.[68] They should help people build digital reflexes such as pausing before clicking links, verifying digital identities or reporting suspicious interactions. Educational content must be immersive, locally tailored and reinforced through schools, workplaces, community programs and public outreach. Simulation exercises and interactive tools can further build confidence and readiness in daily life.

> **In Action 1**
> **Singapore: SGScamWISE[69]**
>
> SG ScamWISE (Well-Informed, Secured and Empowered) is a national education programme in Singapore that aims to equip individuals, with the skills to protect themselves from scams and fraud. Initiated by Bamboo Builders supported by Google.org, the national education programme targets 100,000 Singaporeans by 2026.
>
> Adopting a whole-of-society approach, Bamboo Builders works with Singapore's government agencies to continually update its curriculum, thereby ensuring that the public is aware of the latest scam tactics and knows how to protect themselves and their loved ones. They also work with businesses, banks and professional accounting bodies to educate staff on workplace scams and fraud. Bamboo Builders also educates civil society and the community through social service agencies, grassroot entities, religious organisations and social media ambassadors.
>
> Bamboo Builders has also pushed the envelope on scams awareness education delivery. Beyond information-sharing alone, the programme combines interactive storytelling and real-world case studies into an immersive gamified learning experience. Through empathy-driven education, Bamboo Builders promotes digital literacy, behaviour change and community resilience. e Post-programme, the initiative also encourages individuals to sign up as ambassadors, adopt protective digital habits, build resilience and serve as first responders within their households and wider social networks.

↗ Leverage Trusted Community Voices and Intergenerational Networks

In SEA, trust is often local. Many communities place greater faith in familiar figures such as village heads, religious leaders, or family members than in formal authorities or abstract public messaging. This presents a powerful opportunity to scale scam prevention by partnering with credible local voices and embedding awareness into existing community structures.

Trusted messengers can translate digital risks into locally relevant advice, especially for populations with low formal education or limited internet access. Intergenerational relationships also offer a key entry point: younger people, who are generally more digitally literate, can play a protective role for older family members by teaching them how to identify scams or respond to suspicious messages. Encouraging this mutual learning builds protective habits while fostering family- and community-level resilience.

Idea in Focus 1
Leaning on Religious Leads and Community Leaders in Thailand[70]

In Thailand, roundtable participants emphasised the importance of engaging culturally respected voices–such as monks and local influencers–who are seen as credible sources of information in their communities. These figures can effectively translate anti-scam messages into accessible and relatable guidance. A standout proposal involved empowering youth to educate older family members and neighbours about digital threats. By bridging the generational gap, this approach enables mutual learning: younger people offer practical digital tips, while elders provide local wisdom and contextual insight. Community-based awareness campaigns, including local workshops and school events, have already begun to reinforce these efforts by building grassroots confidence and self-reliance in scam recognition and reporting.

Idea in Focus 2
Harnessing Gotong Royong for Community-Led Scam Prevention in Indonesia[71]

During the Indonesia roundtable, participants proposed drawing on the cultural value of *Gotong Royong*– a principle of mutual aid and collective responsibility–as a foundation for community-led scam prevention. While national systems and enforcement mechanisms are important, participants noted that grassroots solidarity remains a powerful and underutilised resource, especially in rural or lower-income communities. One idea involved establishing "anti-scam circles" led by village elders, where traditional gatherings and storytelling could be used to raise awareness, particularly around scams linked to religious travel. These locally rooted approaches were viewed as more trusted and relatable than formal campaigns, demonstrating how strong systems and strong social bonds can reinforce one another.

4.2. Identify and Detect: Enhancing Scam Detection Across the Ecosystem

The *Identify* pillar focuses on detecting, verifying, and intercepting scam threats in real-time before financial or emotional damage occurs.

Effective detection requires more than just technical infrastructure. In today's digital landscape, where scams are increasingly personalised through AI-generated deepfakes, hijacked social media accounts and spoofed platforms, detection is a race against deception. Combating such threats demands a blend of advanced technological tools, frontline coordination and heightened public vigilance at all times.

Roundtable participants from across the SEA-6 region consistently emphasised that scam detection is a shared responsibility. Financial institutions, telecommunications companies and digital platforms hold valuable data signals that can reveal fraud patterns. Sharing this data is vital. At a global scale, the Global Signal Exchange (GSE), developed by the DNS Research Federation, Google, and the Global Anti-Scam Alliance, offers a useful model.[72] It connects digital economy companies such as Microsoft, Meta, telecoms and security researchers to facilitate secure and near real-time exchange of phishing sites, scam content and spoofed identities.

At the same time, communities and end users provide real-time and on-the-ground intelligence that can validate or flag suspicious activity. The most effective detection systems are those that combine the speed of machines with the contextual awareness of human insight.

The table below illustrates key areas where each segment of the society can contribute to building resilience under the *Identify and Detect* pillar.

Table 3. Identify and Detect: A Whole-of-Society Approach

Stakeholder Group	Potential Roles and Responsibilities in Identify and Detect
Government	• Invest in national scam detection infrastructure, including tools like AI and central databases • Develop and enforce SIM card registration and caller verification laws • Coordinate real-time reporting and intelligence sharing across agencies • Establish and maintain user-friendly public reporting channels • Lead data-sharing protocols across borders and sectors
Businesses	• Build and integrate fraud detection systems (e.g. scam filters, AI screening) • Share scam intelligence with regulators and peer institutions • Provide accessible, in-platform scam reporting tools • Alert users to suspicious activity (e.g. flagged phone numbers and malicious scam pop-ups) • Participate in government-coordinated reporting and data-sharing efforts

Stakeholder Group	Core Roles and Responsibilities in Protection
Civil Society Organisations	• Operate or support community-based scam reporting platforms • Provide technical feedback on detection tools (usability, fairness) • Advocate for inclusive and privacy-safe detection policies • Train local actors to identify and escalate scams • Conduct research on scam trends and detection gaps
Community Networks	• Raise awareness about common scam tactics and how to report • Help vulnerable or less tech-savvy individuals use reporting tools • Share verified alerts and guidance through trusted local channels (e.g. sermons, WhatsApp groups) • Reinforce phone and SMS verification practices within communities
End Users	• Use official reporting tools to flag scams • Adopt scam detection apps and telecom verification features • Share alerts and educate peers or customers • Stay informed about new scam tactics and digital safety updates • Ensure personal devices and SIMs are registered and secured

Source: Tech for Good Institute, 2025

Building on top of these shared responsibilities, there are key actions that can be considered across the region to further strengthen resilience at this stage.

Use Technology-Based Solutions to Combat Scams and Fraudulent Activity

As scams become more sophisticated, technology must serve as the first line of defence in detecting and disrupting fraudulent activity. Across SEA, there is growing momentum to develop systems that use AI, machine learning and advanced analytics to monitor suspicious behaviour, flag anomalies and block threats in real time. These tools are increasingly vital in identifying complex scams, including AI-generated voice calls, deepfakes, spoofed platforms and phishing websites.

At the Malaysia roundtable, participants proposed the use of generative AI tools to proactively scan websites, monitor dark web activity and analyse transaction patterns.[73] Such tools could detect scam indicators, alert users to suspicious links, block robocalls and identify spoofed numbers. AI-driven call screening technologies were also recommended to counter scams involving manipulation and social engineering, such as romance scams.

Similar momentum was noted in Thailand, where the government is exploring AI-based detection tools to monitor financial transactions and e-commerce activity.[74] Participants also highlighted the value of mobile applications that can identify scam phone numbers and flag fraudulent communications as effective, user-facing tools.[75]

Across the discussions, there was broad consensus on the importance of building detection systems that are integrated, accessible, and responsive to fast-changing scam tactics. Public sector leadership is crucial, particularly when complemented by private sector innovation from banks, telcos, fintechs, and digital platforms. These tools must not only detect and block scams, but also empower users with real-time alerts, reporting functions and accessible guidance.

In Action 2
Leveraging Technology-based Solutions[76]

In Singapore, ScamShield represents a coordinated, technology-driven approach to scam detection and prevention. Developed by Open Government Products in collaboration with the Singapore Police Force and the National Crime Prevention Council, the app is part of a broader suite of tools designed to help individuals recognise and block fraudulent activity.

Available on both iOS and Android, the app automatically filters scam calls and SMSes, flags suspicious content using AI-powered classification, and allows users to check messages, phone numbers, and links across platforms such as WhatsApp, Telegram and SMS. It also enables easy reporting of suspected scams, helping authorities to strengthen their databases and overall response efforts.

Complementing the app are a 24/7 helpline (1799), a dedicated resource website, and real-time alerts delivered via WhatsApp. Together, these tools provide an integrated, user-centric system that empowers users, increases public vigilance and reinforces Singapore's broader anti-scam infrastructure as a whole.

Enable Grassroots and Citizen-Driven Reporting and Intelligence

Scam detection cannot rely solely on institutional systems. In many cases, everyday users are the first to encounter new scam tactics, particularly those that evolve quickly or target specific communities. Empowering individuals to report scams easily and ensuring these reports feed into broader fraud intelligence systems can help governments, platforms, and law enforcement track patterns, respond swiftly, and strengthen prevention strategies.

Citizen-driven platforms also play a critical role in building a culture of vigilance. When individuals see their contributions acknowledged and acted upon, public trust improves and reporting becomes more consistent. As highlighted in the Vietnam roundtable, platforms like *ChongLuaDao* demonstrate the potential of grassroots innovation to complement national efforts. With the right partnerships, such models can be scaled and integrated into wider detection frameworks to enhance detection, accelerate response, and embed scam prevention across society.

Vietnam's ChongLuaDao, a platform led by a non-profit organisation, has emerged as a notable grassroots initiative in the fight against scams. The platform enables the public to report suspicious activities, supports community-based verification and facilitates threat intelligence sharing, while also running awareness campaigns to improve digital safety and vigilance.

During the roundtable, participants highlighted the importance of scaling such efforts through structured collaboration between civil society, government, private sector actors and digital platforms. Key opportunities includes:

• Government agencies encouraging public reporting and integrating data into ChongLuaDao's systems.

• The private sector, particularly fintech companies and telecom providers, supporting AI-powered scam detection and embedding scam alerts into user-facing interfaces.

• Digital platforms amplifying anti-scam content and enabling peer-to-peer alert sharing at scale for greater impact.

To sustain and scale such initiatives, participants recommended formalising cross-sector partnerships, positioning grassroots reporting as a core element of Vietnam's national digital resilience strategy. In doing so, scam prevention becomes a shared and coordinated responsibility across the digital ecosystem.

Strengthen Caller and SMS Verification Systems

Scams conducted through spoofed calls and phishing SMS messages remain a widespread threat across SEA.[78] These attacks often exploit weaknesses in the telecommunications ecosystem, particularly unregistered SIM cards and unsecured messaging systems. Roundtable participants across several countries emphasised the need for stronger verification systems and enforcement measures that improve the traceability of digital communications and reduce opportunities for fraud.

Authorities in Thailand are moving to regulate bulk SIM card purchases to curb call centre scams, following the police seizure of 200,000 SIM cards linked to a Chinese scam syndicate.[79] At present, there are no restrictions on corporate entities buying SIMs in bulk for resale, aside from a rule requiring individuals with more than five numbers to register them. The National Broadcasting and Telecommunications Commission (NBTC) plans to implement changes gradually to minimise disruption to consumers and businesses.

In Malaysia, the government is strengthening its collaboration with the telecommunications companies to improve SIM card verification through the MyDigital ID platform as part of its efforts to reduce cybercrime.[80] Under this initiative, users will be required to verify their identity using MyDigital ID when registering a new SIM card or reactivating an existing one. This measure aims to prevent fraudulent SIM card registrations and make it more difficult for scammers to use unauthorised or stolen identities.

A consistent message across the roundtables was the importance of an integrated approach: verification systems must be backed by enforcement, public education and real-time coordination between telecoms, financial institutions, and regulators.

In Action 4
Strengthening the SIM Card Registration in the Philippines[81]

In the Philippines, SIM card registration has emerged as a critical area of reform in efforts to combat online scams. Under Republic Act 11934, signed into law in 2022, all users are required to register their SIM cards to reduce anonymity and curb cybercrime. However, stakeholders have raised concerns about major loopholes in implementation, particularly the absence of a cap on the number of SIMs one person can register.

During recent discussions, Scam Watch Pilipinas revealed that individuals involved in scam operations had registered up to 600 SIM cards each, enabling large-scale fraud. The Philippines National Police Anti-Cybercrime Group (PNP ACG) reported over 600 arrests linked to violations such as selling pre-registered SIMs. Both the Department of Information and Communications Technology (DICT) and civil society have proposed limits on SIM ownership—ranging from three to ten per person—to balance individual, business, and family needs. These reforms are seen as essential to strengthening enforcement, improving traceability and reducing the misuse of telecom infrastructure in scam operations.

4.3. Respond and Recover: Scaling Response and Enhancing Recovery Support

The *Respond and Recover* **pillar focuses on enhancing society's capacity to act swiftly and effectively after a scam has occurred.** While proactive measures help reduce exposure, no system is entirely immune. When scams do happen, timely intervention and victim-centred recovery are essential. This includes establishing clear reporting pathways, enabling coordinated enforcement, and ensuring that victims receive comprehensive and compassionate support.

Effective response and recovery not only help disrupt ongoing scams but also play a vital role in restoring trust and emotional well-being of victims. Achieving this requires cross-sector collaboration to ensure that cases are escalated efficiently, fraudulent operations are dismantled, and affected individuals are guided through a clear, supportive recovery process. The table below outlines the potential areas of contributions of each stakeholder group under the *Respond and Recover* pillar.

Table 4. Respond and Recover: A Whole-of-Society Approach

Stakeholder Group	Potential Roles and Responsibilities in Respond and Recover
Government	• Establish integrated, multi-agency scam response centres • Mandate case escalation pathways and shared investigation frameworks • Enable real-time law enforcement coordination across jurisdictions • Fund victim support services, including mental health care
Businesses	• Participate in scam response centres (banks, telcos, platforms) • Provide immediate account freezes and "kill switch" features for victims • Share fraud data with law enforcement and peer institutions • Cooperate on cross-border scam investigations • Support victim care through account recovery and claims processes
Civil Society Organisations	• Provide legal aid, counselling, and referral services to scam victims • Train frontline staff to support trauma-informed responses • Act as public educators on how to escalate scam cases • Monitor enforcement and recovery outcomes for transparency • Advocate for victim-centred response policies
Community Networks	• Serve as local escalation points, particularly in rural or low-access areas • Support scam victims emotionally and practically during recovery • Reinforce reporting pathways and support group structures • Help raise awareness about what to do immediately after a scam
End Users	• Report scams via official channels and encourage others to do the same • Use available support services and participate in peer support groups • Cooperate with investigators by preserving evidence • Stay updated on recovery tools and procedures • Help destigmatise victimhood by sharing experiences

Source: Tech for Good Institute, 2025

Based on the regional roundtables, participants highlighted key areas of recommendation that countries can pursue to strengthen resilience in the area of response and recovery.

↗ Establish Coordinated Response through National Scam Centres

Fragmented reporting systems weaken public trust and delay effective action. In many cases, victims are unsure where to report scams, receive inconsistent guidance, or face poor coordination between law enforcement, banks and telecommunications providers. This issue was especially evident in the Philippines and Indonesia roundtables, where participants highlighted how overlapping mandates and unclear responsibilities create confusion around scam response procedures.

Establishing a national scam centre can help address these gaps by providing a single, integrated entry point for scam reports. Such centres facilitate real-time coordination and ensure that cases are routed efficiently to the appropriate agencies. They also enable cross-sector information sharing, helping stakeholders respond more swiftly and accurately to emerging threats.

One of the key best practices identified during the roundtables is the co-location of core stakeholders. This includes embedding the police, financial institutions, telecommunications companies, digital platforms and regulators within a unified response team.

> ### In Action 5
> ### Co-location of Key Stakeholders in Singapore's Anti-Scam Command[82]
>
> Singapore's Anti-Scam Command (ASCom), established in March 2022 under the Singapore Police Force, is a centralised unit dedicated to coordinating and strengthening the national response to scams. By consolidating investigation, enforcement, incident response, and intelligence within a single structure, ASCom enables rapid intervention and proactive disruption of scam operations.
>
> A key feature of its success is the physical co-location of stakeholders, including officers from major banks such as DBS, OCBC, UOB, Standard Chartered, HSBC and CIMB, who work alongside police to trace and freeze scam-related funds in real time. This setup has significantly reduced turnaround times for freezing suspicious accounts, from days to mere hours or minutes, which has improved the chances of recovering stolen assets. ASCom also partners with e-commerce platforms like Carousell and Shopee and agencies such as GovTech to investigate cases involving digital identity fraud.

Strengthen Law Enforcement Coordination Across Borders

While national efforts remain critical, scam operations often span multiple jurisdictions, making regional cooperation essential for timely disruption and effective asset recovery. However, many agencies still face gaps in cybercrime training, digital forensics capabilities and legal authorisation that limit their ability to respond.

To address these challenges, governments must invest in equipping their law enforcement agencies with the right tools, specialised personnel, and cross-border frameworks for collaboration. This includes strengthening bilateral and multilateral agreements, creating shared protocols for investigation and evidence sharing, and building trusted networks for joint operations. Effective law enforcement coordination also depends on clearly defined escalation pathways and a commitment to sustained information exchange between countries.

In Action 6 box below showcases a sample of cross-border collaboration on scam response and asset recovery.

In Action 6
Advancing Cross-Border Collaboration on Scam Response and Asset Recovery[83]

Launched in October 2024 by the Singapore Police Force, FRONTIER+ brings together anti-scam agencies from Hong Kong SAR, Malaysia, Maldives, South Korea and Thailand to tackle cross-border scam operations. The initiative focuses on disrupting illicit networks, recovering assets for victims, and building regional capabilities through the exchange of best practices.

By strengthening cooperation across jurisdictions, FRONTIER+ enhances the region's ability to respond to transnational scam threats. In one example of its impact, Singapore's Anti-Scam Command worked with Malaysia's National Scam Response Centre to recover around USD 90,000 from an investment scam case in December 2024.

Support Victims with Psychosocial Care

Scam victims often experience more than just financial loss. Emotional distress, feelings of shame, social isolation, and psychological trauma are common, particularly in scams that exploit personal trust, such as romance fraud, family impersonation, and investment scams. Roundtable discussions across the SEA-6 countries consistently highlighted the importance of integrating structured, victim-centred care into national response systems. Participants from the Philippines, Malaysia and Vietnam emphasised the need for trained personnel within reporting hotlines, escalation protocols for urgent cases and accessible psychosocial support services for scam victims.

Victim care must be central to any effective scam response system. Stakeholders advocated for national-level programmes that provide trauma-informed care through trained personnel who can guide victims through reporting processes, offer emotional support and ensure access to legal and financial assistance. Proposals included staffing national scam response centres with trained call operators, integrating mental health support within law enforcement procedures and establishing clear referral pathways to professional counselling services. The overarching goal is to ensure victims receive consistent, compassionate support throughout their recovery, while reducing stigma and encouraging timely reporting.

Singapore's Victim Care Officer (VCO) Programme, led by the Singapore Police Force, provides personalised, trauma-informed support to victims of crime, including those affected by scams. The programme engages trained volunteers with backgrounds in counselling, psychology or social work, who guide victims through the criminal justice process, offering both emotional reassurance and practical assistance. VCOs are selected through a rigorous screening process, including interviews, psychometric assessments, and specialised training. From the point of first contact, VCOs help victims understand investigative procedures, manage trauma, and, when necessary, connect them to community services and mental health support. By offering consistent care during investigations and legal proceedings, the programme plays a key role in ensuring victims receive holistic support throughout their recovery.

4.4. Adapt: Building Resilience for the Future

The *Adapt* pillar focuses on strengthening the long-term capacity of societies to stay ahead of emerging and evolving scam threats. Beyond immediate prevention and response, adaptation requires institutions to be agile, legal systems to be responsive and regional cooperation mechanisms to be proactive and future-ready. This includes regularly stress-testing national systems, identifying and closing legal and regulatory loopholes and scaling up successful anti-scam solutions across different sectors and borders.

Roundtable discussions across the SEA-6 countries highlighted a clear consensus: adaptation is essential to digital resilience. The ability to learn from past incidents, rapidly adjust policies and practices, and anticipate new scam tactics is crucial in an environment where cyber threats are constantly evolving. Building this adaptive capacity requires the active participation of the entire ecosystem, including governments, businesses, civil society, community networks and end users. Each group has a unique role to play in ensuring that anti-scam measures remain effective, inclusive and forward-looking.

The table below outlines the specific ways in which different stakeholders can contribute to fostering adaptation, supporting a more resilient and responsive digital environment for the region.

Table 5. Adapt: A Whole-of-Society Approach

Stakeholder Group	Potential Roles and Responsibilities in Adaptation
Government	• Lead scenario planning and national scam simulations • Continuously update laws in response to scam evolution • Coordinate regional harmonisation of cyber and consumer protection policies • Use chairmanships and forums (e.g. ASEAN) to advance cross-border cooperation on key issues • Invest in legal foresight and regulatory sandboxes
Businesses	• Collaborate on simulation drills and user safety testing • Advocate for practical regulatory updates and compliance alignment • Integrate adaptive scam protection features based on emerging tactics • Scale tested solutions (e.g. scam alerts, verification systems) across markets • Participate in regional data sharing and standard-setting bodies
Civil Society Organisations	• Help design and run scam drills in schools and communities • Advocate for legal reforms to protect vulnerable groups • Monitor emerging scam patterns and policy gaps • Bridge research, policy, and public education through adaptive toolkits • Engage in regional civil society networks for shared learning
Community Networks	• Support local participation in national drills and simulations • Help test and provide feedback on policy or tool rollouts • Share local intelligence on scam adaptations • Advocate for inclusive adaptation measures that reflect rural or marginalised perspectives in policymaking
End Users	• Participate in drills, trainings, and simulations • Adopt updated tools and follow revised safety protocols • Stay informed about new threats and evolving scam tactics • Share experiences and feedback to improve future adaptations • Engage in civic dialogue on rights, protection, and digital responsibility

Source: Tech for Good Institute, 2025

Insights from the regional roundtables identified priority recommendations that countries can adopt to enhance their capacity for adapting to the evolving scams and fraud landscape in SEA.

↗ Consider National Scam Drills as Public "Digital Vaccines"

Scam drills offer a proactive way to strengthen behavioural resilience. Similar to fire drills that prepare individuals for physical emergencies, scam drills expose users to simulated fraud scenarios in a safe, educational setting. This approach helps individuals build practical reflexes and greater confidence in identifying scams before they encounter them in real situations. The concept gained particular support in Vietnam, where stakeholders described scam drills as a form of "scam vaccine" that instils protective behaviours early and effectively.

Participants suggested incorporating scam drills into schools, universities, workplaces, and public institutions, using both online and offline formats. Exercises could include phishing simulations, mock job offers or impersonation calls. Additionally, digital platforms and fintech companies could adopt such tools during onboarding or promotional campaigns to reinforce scam recognition skills among users.

Idea in Focus 3 highlights an illustrative example of this approach through a game-based intervention, demonstrating how experiential learning can strengthen scam detection and preparedness against online threats.

Idea in Focus 3
Game-based Interventions as Scam Drills to Drive Resilience[85]

Stakeholders strongly supported the use of scam drills and controlled simulations as a proactive way to build resilience against scams. These exercises expose individuals to simulated scam scenarios in a safe, educational setting, functioning like a "scam vaccine" by helping users recognise manipulation tactics before encountering them in real life. This approach draws on active, experiential learning, which focuses on understanding the psychology of scams and has been shown to build stronger resistance than passive warnings alone.

One example of this method is the Be Scam Ready initiative (formerly known as ShieldUp!).[86] In a pilot randomised controlled trial involving 3,000 participants in India, players demonstrated significant and sustained improvements in recognising scam scenarios for up to 21 days after the intervention. Participants who played the game outperformed those who had only watched 10 to 15 minutes of traditional awareness videos or online safety tips. Notably, this heightened scam detection ability did not result in unnecessary distrust of legitimate online interactions. This is a potential model that can be explored by countries in SEA.

Close Systemic Gaps by Updating Related Legislations

Scammers frequently exploit legal and regulatory loopholes, taking advantage of outdated or fragmented laws. These weaknesses are not limited to digital regulations but extend across various sectors, including business registration, labour protection and financial governance. Roundtable discussions across SEA consistently highlighted the need for countries to adopt a more comprehensive legal strategy that keeps pace with evolving scam tactics.

Governments should undertake regular legislative audits to review and update laws across all relevant sectors, closing gaps that allow fraudulent activity to flourish. This includes strengthening traceability, enhancing accountability for digital platforms, and protecting vulnerable groups such as gig workers, migrants and youth. Testing reforms through regulatory sandboxes may also support more agile and responsive legislation. Idea in Focus 4 below illustrates how discussions from stakeholders in Malaysia note the importance of tackling business registration laws, consumer protection laws and human trafficking laws exploited by scam networks.

Idea in Focus 4
Close Systemic Loopholes Through Holistic Legal Reform in Malaysia[87]

Stakeholders In Malaysia, stakeholders stressed the need for a more comprehensive legal response to address the rising sophistication of scam operations. While recent initiatives such as the Cybersecurity Act 2024 mark positive steps, roundtable discussions revealed significant gaps across the broader legal framework.

Participants called for a holistic approach that goes beyond consumer protection and digital economy laws to tackle vulnerabilities in company registration, labour protections and financial regulations. Company registration processes were flagged as a key loophole, with scammers able to repeatedly set up fraudulent businesses under new names.

There were also strong calls to update human trafficking laws to address job scams linked to forced labour, referencing cases where Malaysians had to be rescued from scam compounds. To keep pace with evolving threats, stakeholders recommended regular legislative audits to identify and update outdated provisions across sectors. This comprehensive reform, combined with strengthened enforcement, was viewed as essential to closing systemic loopholes exploited by organised scam networks.

5.
Sustaining Digital Resilience for Southeast Asia's Future

This report examined how digital resilience against digitally-enabled scams and fraud requires a Whole-of-Society Approach to foster a safer and more trusted digital environment. As Southeast Asia continues its rapid digital transformation, such resilience is an enabler of inclusive growth by maintaining trust amongst users. The following principles can guide the innovation, design and implementation of resilience-building measures.

First, shared responsibility and a whole-of-society approach reinforce digital resilience. As stressed in this report, resilience cannot rest with only a few institutions or sectors. Rather, each stakeholder plays a clear and complementary role. The accountability and responsibility should also be shared across the entire ecosystem. For example, governments can set the policy direction and establish national infrastructure for digital safety. Businesses can design platforms that implement safety-by-design features into their applications. Civil society and academic institutions are well-positioned to lead public education, support marginalised groups and contribute research to inform policy. In addition, community leaders and individual users play a critical role in preventing scams by spreading awareness and encouraging safer online behaviour. These efforts create an enabling environment where users can make informed decisions and contribute to the collective resilience of the digital economy as a whole.

Second, innovation plays a critical role in sustained adaptation to the evolving threat landscape. Scam will continue to evolve in complexity and sophistication. We need innovation to anticipate and adapt to these risks to stay ahead. This requires ongoing investment in technology solutions, from AI-powered detection tools to user verification systems. The environment for innovation can benefit from flexible governance, such as the use of regulatory sandboxes.

Third, resilience efforts must remain people-centred and be relevant to the lived realities of local society. Digital safety interventions must be relevant, relatable, and responsive to the everyday realities of users. SEA is diverse, so there is no single roadmap for scam management or digital resilience. This means designing awareness campaigns in local languages, working through trusted community figures, and building solutions that reflect cultural values and communication styles. Localisation is not an afterthought. It is essential to ensure that efforts reach those who are most vulnerable and resonate with communities at every level. This also goes a long way not only in awareness, but also in adoption of resilience-building techniques.

Finally, regional coordination and global cooperation is essential. Scams increasingly operate across borders, taking advantage of jurisdictional gaps and fragmented enforcement. SEA must strengthen regional cooperation through shared intelligence, harmonised laws, and joint enforcement mechanisms. ASEAN can play a central role by facilitating cross-border dialogue, enabling multilateral investigations and supporting the recovery of assets for scam victims. Regional responses are not a replacement for national action, but a necessary extension of it in an interconnected digital landscape.

References

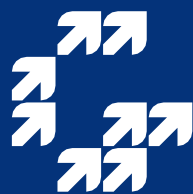|	References
1	Hoppe, F., Baijal, A., Chang, W., Chadna, S., & Hoong, F. W. (2023). *E-Conomy SEA 2023.* Google, Temasek, and Bain & Company. Retrieved June 25, 2025 from https://web.archive.org/web/20250716084859/https://services.google.com/fh/files/misc/e_conomy_sea_2023_report.pdf
2	Tech for Good Institute. (2023, June). *From "Tech for Growth" to Tech for Good".* Retrieved June 25, 2025, from https://web.archive.org/web/20240903023121/https://techforgoodinstitute.org/wp-content/uploads/2023/07/TFGI_TFG_Report_Digital_report.pdf
3	World Economic Forum. (2023). *Global Risks Report 2024 (19th Edition).* Retrieved June 25, 2025, from https://web.archive.org/web/20250716085838/https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
4	Devaraj, S. (2024, December 12). Who is UNC3886, the group that attacked Singapore's critical information infrastructure?. Retrieved July 30, 2025, from https://web.archive.org/web/20250813032829/https://www.straitstimes.com/singapore/who-is-unc3886-the-group-that-attacked-spores-critical-information-infrastructure
5	Singapore Police Force. (2025, February 25). Annual scams and cybercrime brief 2024. Public Affairs Department, Singapore Police Force. Retrieved June 25, 2025, from https://web.archive.org/web/20250620140607/https://www.scamshield.gov.sg/files/Scams%20and%20Cybercrime%20Briefs/2024_annual_scams_and_cybercrime_brief.pdf
6	Vietnam Plus. (2024, January 8). *Vietnamese loss 16.23 billion USD to online scams.* Retrieved June 25, 2025, from https://web.archive.org/web/20250813033339/https://en.vietnamplus.vn/vietnamese-loss-1623-billion-usd-to-online-scams-post276711.vnp
7	United Nations Office on Drugs and Crime. (2024). *Transnational organized crime convergence report 2024.* Retrieved June 25, 2025, from https://web.archive.org/web/20250813033529/https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf
8	Octavia, J. (2025, January 3). *Addressing legal ambiguities and regulatory gaps: Defining online fraud and scams in Indonesia.* Tech for Good Institute. Retrieved June 25, 2025 from https://web.archive.org/web/20250815092522/https://techforgoodinstitute.org/blog/country-spotlights/addressing-legal-ambiguities-and-regulatory-gaps/
9	Ibid.
10	Singapore Statutes Online. (2020). Penal Code [Penal Code 1871 ss. 415–420A]. Attorney-General's Chambers. Retrieved June 25, 2025 from https://sso.agc.gov.sg/act/pc1871?ProvIds=pr415-,pr416-,pr416A-,pr417-,pr418-,pr419-,pr420-,pr420A-
11	Singapore Parliament. (2024). Protection from Scams Bill 43 of 2024. Retrieved June 25, 2025 from http://web.archive.org/web/20250620192734/https://www.parliament.gov.sg/docs/default-source/bills-introduced/protection-from-scams-bill-43-2024.pdf?sfvrsn=e85b5008_1
12	Respicio, H. (2025, March 17). Penalties under RPC Articles 315 and 318 for estafa. Respicio & Co. Law Firm. Retrieved June 25, 2025 from http://web.archive.org/web/20250815100159/https://www.respicio.ph/commentaries/penalties-under-rpc-articles-315-and-318-for-estafa
13	Respicio, H. (2024, October 14). Legal advice and overview on fraud in the Philippines. Respicio & Co. Law Firm. Retrieved June 25, 2025 from https://web.archive.org/web/20250815095852/https://www.lawyer-philippines.com/articles/legal-advice-and-overview-on-fraud-in-the-philippines

14	Siam Legal International. (n.d.). Criminal Code: Fraud (Sections 341–348). Thailand Law Library. Retrieved June 25, 2025 from https://web.archive.org/web/20250815094637/https://library.siam-legal.com/thai-law/criminal-code-fraud-sections-341-348/
15	Nasaruddin, N. I. D. (2020, July 14). Legal implications and remedies in relation to common business scams in 2020. A Z Milaw & Associates. Retrieved 25 June 2025 from https://web.archive.org/web/20250815094526/https://www.azmilaw.com/insights/legal-implications-remedies-in-relation-to-common-business-scams-in-2020/
16	Raja Ahmad Aminollah, R. N. A., & Lim, T. K. H. (2022, December 1). An overview of the law on fraudulent trading in Malaysia. Skrine. Retrieved 25 June 2025 from https://web.archive.org/web/20250815094508/https://www.skrine.com/insights/alerts/december-2022/an-overview-of-the-law-on-fraudulent-trading-in-ma
17	Nguyen, P. H. T. (2024, April 19). Penalties for imposter scams in Vietnam. LawNet Vietnam. Retrieved June 25, 2025, from https://web.archive.org/web/20250815094454/https://lawnet.vn/judgment/en/tin-tuc/penalties-for-imposter-scams-in-vietnam-10142
18	Ibid.
19	HSBC UK. (n.d.). *Fraud and scams: How To Spot The Difference.* Retrieved June 25, 2025 from https://web.archive.org/web/20250801022720/https://www.hsbc.co.uk/help/security-centre/fraud-guide/difference-between-fraud-and-scams/
20	PayPal US. (2023). *Fraud vs Scams: How Are They Different?* Retrieved June 25, 2025 from https://web.archive.org/web/20250801022809/https://www.paypal.com/us/money-hub/article/fraud-vs-scam-difference
21	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
22	Monihuldin, M. (2023, April 21). QuickCheck: Are scammers phishing Telegram users with fake bank websites?. *The Star.* Retrieved June 25, 2025, from https://web.archive.org/web/20250715103127/https://www.thestar.com.my/news/true-or-not/2023/04/21/quickcheck-are-scammers-phishing-telegram-users-with-fake-bank-websites
23	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
24	Fischer, P., Lea, S. E. G., & Evans, K. (2009). The psychology of scams: Provoking and committing errors of judgement. *Trends in Cognitive Sciences,* 13(1), 42–49. https://doi.org/10.1016/j.tics.2008.11.003
25	VietnamNet Global. (2024, July 1). Impersonation scams: A growing threat in Vietnam and globally. *VietnamNet.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716090854/https://vietnamnet.vn/en/impersonation-scams-a-growing-threat-in-vietnam-and-globally-2296843.html
26	Federal Trade Commission. (n.d.). *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
27	SCMP's Asia Desk. (2025, February 3). Woman arrested in Thailand over record US$186 million romance scam. *South China Morning Post.* Retrieved June 25, 2025, from https://web.archive.org/web/20250210105440/https://www.scmp.com/week-asia/people/article/3297216/woman-arrested-thailand-over-record-us186-million-romance-scam
28	CelcomDigi. (2024, August 5). *Fake friend scam.* Retrieved June 25, 2025, from https://web.archive.org/web/20250715104815/https://help.celcomdigi.com/support/solutions/articles/70000657780-fake-friend-scam

29	Art by Rhia. (2025, June 14). An Indonesian university student described a "fake friend" scam involving compromised Facebook accounts belonging to real friends, requests for urgent surgery payments, and proof-of-transfer demands. *Facebook.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716091538/https://www.facebook.com/groups/facebooksleuthsdeconstructingscammers/posts/1210072950442137/
30	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
31	Bureau of Immigration (Philippines). (n.d.). *Telegram and Facebook used by syndicates to lure trafficking victims to work for scam hubs.* Retrieved June 25, 2025, from https://web.archive.org/web/20250406030907/http://immigration.gov.ph/telegram-and-facebook-used-by-syndicates-to-lure-trafficking-victims-to-work-for-scam-hubs/
32	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/
33	Kaushik, P., Garg, V., Priya, A., & Kant, S. (2024). Financial fraud and manipulation: The malicious use of deepfakes in business. In *Deepfakes and their impact on business* (pp. 173–196). IGI Global. https://doi.org/10.4018/979-8-3693-6890-9.ch008
34	Cyber Security Agency of Singapore. (2024, March 22). *Advisory on detecting and responding to deepfake scams.* Retrieved June 25, 2025, from https://web.archive.org/web/20250610212857/https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2024-006
35	Tech For Good Institute. (2025, May 14). Building resilience against scams and fraud: Spotlight on Philippines. Retrieved June 25, 2025, from https://web.archive.org/web/20250716064635/https://techforgoodinstitute.org/blog/event-highlights/building-resilience-against-scams-and-fraud-spotlight-on-philippines/
36	United Nations Office on Drugs and Crime (UNODC). (2024*). Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden, accelerating threat.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716064048/https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf
37	Sumsub. (2023, November 28). *Sumsub Research: Global deepfake incidents surge tenfold from 2022 to 2023.* Retrieved June 25, 2025, from https://web.archive.org/web/20250714022520/https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/
38	Dickson, J., & Preputnik, L. B. (2025). *Cyber scamming goes global: Unveiling Southeast Asia's high-tech fraud factories.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716064311/https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories
39	Rogers, S. (2024, September 25). 37 billion reasons the citizens of Malaysia, Taiwan, and Thailand need better scam protection. *GASA.* Retrieved June 25, 2025, from https://web.archive.org/web/20250429172549/https://www.gasa.org/post/where-did-the-billions-go-in-malaysia-thailand-taiwan
40	Bamboo Builders. (2025, March). *Strengthening scam readiness in Singapore: March 2025.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716065040/https://www.bamboobuilders.org/_files/ugd/ebb12b_84abfb289d624a618716ff4d3a17879c.pdf
41	Ibid.
42	Tech for Good Institute. (2025, April 14). *Building resilience against scams and fraud: Spotlight on Malaysia.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716065212/https://techforgoodinstitute.org/blog/event-highlights/building-resilience-against-scams-and-fraud-spotlight-on-malaysia/

43	Luong, H. T. (2025, May 19). *From fake jobs to crypto fraud: Why scam gangs in Southeast Asia are a growing global threat.* Griffith University. Retrieved June 25, 2025, from https://web.archive.org/web/20250716065313/https://blogs.griffith.edu.au/gci-insights/2025/05/19/from-fake-jobs-to-crypto-fraud-why-scam-gangs-in-southeast-asia-are-a-growing-global-threat/
44	Luong, H. T. (2025, March 14). *Collaboration crucial to combatting scams in Southeast Asia.* East Asia Forum. Retrieved June 25, 2025, from https://web.archive.org/web/20250716065418/https://eastasiaforum.org/2025/03/14/collaboration-crucial-to-combatting-scams-in-southeast-asia/
45	Beh, M. T. (2025, March 19). *Combating scam syndicates in Malaysia and Southeast Asia.* Penang Institute. Retrieved June 25, 2025, from https://web.archive.org/web/20250716065520/https://penanginstitute.org/publications/issues/combating-scam-syndicates-in-malaysia-and-southeast-asia/
46	Mateo, J. (2024, June 21). *SIM registration law failed to curb scams – group.* The Philippine Star. Retrieved June 25, 2025, from https://web.archive.org/web/20250716065613/https://www.philstar.com/nation/2024/06/21/2364394/sim-registration-law-failed-curb-scams-group
47	United Nations Educational, Scientific and Cultural Organization (UNESCO). (2023). *The United Nations World Water Development Report 2023.* United Nations Educational, Scientific and Cultural Organization. Retrieved June 25, 2025, from https://doi.org/10.18356/9789210026208c021
48	Ibid.
49	Southeast Asia Public Policy Institute. (2024, March 20). Policy State of Play – Online Fraud in Southeast Asia. Retrieved June 25, 2025, from https://web.archive.org/web/20250716070334/https://seapublicpolicy.org/wp-content/uploads/2024/03/SEAPPI-OF-regional-snapshot_14032024-1.pdf#page=1.00
50	Leesa-nguansuk, S. (2025, April 13). New law holds banks, telecoms, social media companies responsible for scams. Bangkok Post. Retrieved June 25, 2025, from https://web.archive.org/web/20250716070434/https://www.bangkokpost.com/business/general/3002366/new-law-holds-banks-telecoms-social-media-companies-responsible-for-scams
51	Monetary Authority of Singapore (MAS). (2023, October 24). *Guidelines on Shared Responsibility Framework.* Retrieved June 25, 2025, from https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework
52	Bangko Sentral ng Pilipinas (BSP). (2024, July 20). *BSP welcomes passage of anti-financial account scamming law.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716072446/https://www.bsp.gov.ph/SitePages/MediaAndResearch/MediaDisp.aspx?ItemId=7179
53	Wu, L. (2024, December 16). *Fraud with Danger: The Rise of Cyber Scams in Southeast Asia. Fulcrum.* Retrieved June 25, 2025, from https://web.archive.org/web/20250530085406/https://fulcrum.sg/aseanfocus/fraud-with-danger-the-rise-of-cyber-scams-in-southeast-asia/
54	Philippines News Agency. (2023, August 14). *Netizens urged to save gov't anti-scam response hotline 1326.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716072624/https://www.pna.gov.ph/articles/1207775
55	Hagenus, S. (2024, November 28). *Beyond legislation: How businesses can build resilient cybersecurity frameworks.* Cyber Security Asia. Retrieved June 25, 2025, from https://web.archive.org/web/20241203060331/https://cybersecurityasia.net/cybersecurity-steps-against-fraud/
56	Tech For Good Institute. (2024, August). *Leveraging digital platforms for public benefit.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716073040/https://techforgoodinstitute.org/wp-content/uploads/2024/08/TFGI_Leveraging-Digital-Platforms-for-Public-Benefit-Report.pdf
57	Bamboo Builders. (n.d.). *SG Scam Wise: A national education programme empowering 100,000 Singaporeans against scams.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716073339/https://www.bamboobuilders.org/sgscamwise

58	Tan, G. (2025, April 4). *Building a scam-resilient Singapore through empathy-led education.* Tech For Good Institute. Retrieved June 25, 2025, from https://web.archive.org/web/20250716073459/https://techforgoodinstitute.org/research/ecosystem-resources/building-a-scam-resilient-singapore-through-empathy-led-education/
59	Bamboo Builders. (2025, March).
60	Tech For Good Institute. (2024, November 4). *Collective action for scam resilience in Southeast Asia.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716074006/https://techforgoodinstitute.org/blog/event-highlights/collective-action-for-scam-resilience-in-southeast-asia/
61	Renshaw, A. (2021, January 28). *The 3 stages of fraud lifecycle.* Feedzai. Retrieved June 25, 2025, from https://web.archive.org/web/20250716075801/https://www.feedzai.com/blog/fraud-attack-lifecycle/#the-lifecycle-of-a-fraud-attack
62	Block, Inc. (2025, January 31). *The life cycle of scams.* Retrieved June 25, 2025, from https://block.xyz/inside/the-life-cycle-of-scams
63	United Nations Development Programme (UNDP). (2024). *Anti-Scam Handbook v1.0: Collective response and tools to safeguard development.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716074642/https://www.undp.org/sites/g/files/zskgke326/files/2024-10/undp_anti-scam_handbook_v1.0.pdf
64	Ibid.
65	Detros, K. (2023, May). *Towards a resilient cyberspace in Southeast Asia.* Tech For Good Institute. Retrieved June 25, 2025 from https://web.archive.org/web/20250704053336/https://techforgoodinstitute.org/wp-content/uploads/2023/07/TFGI_Cybersecurity_Report_Digital_report.pdf
66	Rogers, S. (2024, September 25).
67	Kemp, S. (2024, February 23). *Digital 2024: Vietnam.* DataReportal. Retrieved June 25, 2025, from https://web.archive.org/web/20250716080441/https://datareportal.com/reports/digital-2024-vietnam
68	Christiano, A., & Neimand, A. (2017). *Stop raising awareness already.* Stanford Social Innovation Review. Retrieved June 25, 2025, from https://web.archive.org/web/20250520053453/https://ssir.org/articles/entry/stop_raising_awareness_already
69	Bamboo Builders (n.d.).
70	Tech For Good Institute. (2025, May 22). *Building resilience against scams and fraud: Spotlight on Thailand.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716081006/https://techforgoodinstitute.org/blog/event-highlights/building-resilience-against-scams-and-fraud-spotlight-on-thailand/
71	Ibid.
72	DNS Research Federation (2025). Microsoft, Meta and others join the Global Signal Exchange (GSE). Retrieved June 25, 2025, from https://web.archive.org/web/20250422215600/https://dnsrf.org/blog/microsoft--meta-and-others-join-the-global-signal-exchange--gse-/index.html
73	Tech For Good Institute. (2025, April 14). Building resilience against scams and fraud: Spotlight on Malaysia [Event highlights]. Retrieved June 25, 2025, from https://web.archive.org/web/20250716081149/https://techforgoodinstitute.org/blog/event-highlights/building-resilience-against-scams-and-fraud-spotlight-on-malaysia/
74	Leesa-nguansuk, S. (2025, March 18). *Thailand moves fast to roll out AI for fraud detection.* Bangkok Post. Retrieved June 25, 2025, from https://web.archive.org/web/20250716081351/https://www.bangkokpost.com/business/general/2982171/thailand-moves-fast-to-roll-out-ai-for-fraud-detection

75	Tech For Good Institute. (2025, May 22).
76	Ibid.
77	ChongLuaDao. (n.d.). *ChongLuaDao*. Retrieved June 25, 2025, from https://web.archive.org/web/20250716083514/https://chongluadao.vn/
78	Tang, S. K. (2022, January 21). *'Incredibly easy to spoof': How SMS scams work and what can be done.* Channel News Asia. Retrieved June 25, 2025, from https://web.archive.org/web/20250716081602/https://www.channelnewsasia.com/singapore/sms-phishing-scams-ocbc-fake-messages-2444446
79	Tortermvasana, K. (2024, December 25). *SIM card bulk buying rules to curb scams.* Bangkok Post. Retrieved June 25, 2025, from https://web.archive.org/web/20250716081649/https://www.bangkokpost.com/business/general/2927005/sim-card-bulk-buying-rules-to-curb-scams
80	Parzi, M. N. (2025, March 3). *Govt, telcos tighten SIM verification, MyDigital ID to curb cybercrime.* New Straits Times. Retrieved June 25, 2025, from https://web.archive.org/web/20250716081756/https://www.nst.com.my/news/nation/2025/03/1183113/govt-telcos-tighten-sim-verification-mydigital-id-curb-cybercrime#google_vignette
81	Inquirer.net. (2025, June 25). *Watchdog renews push to limit SIM registration per person to fight scams.* Philippine Daily Inquirer. Retrieved June 25, 2025, from https://web.archive.org/web/20250716081928/https://newsinfo.inquirer.net/2074507/watchdog-renews-push-to-limit-sim-registration-per-person-to-fight-scams
82	Singapore Police Force. (2022, September 6). *Opening of Anti-Scam Command Office.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716082732/https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scam_command_office
83	Singapore Police Force. (2025, February 25). *Annual scams and cybercrime brief 2024.* Retrieved June 25, 2025, from https://web.archive.org/web/20250620140607/https://www.scamshield.gov.sg/files/Scams%20and%20Cybercrime%20Briefs/2024_annual_scams_and_cybercrime_brief.pdf
84	Singapore Police Force. (n.d.). *Victim Care Cadre Programme.* Retrieved June 25, 2025, from https://web.archive.org/web/20250716082917/https://www.police.gov.sg/Join-SPF/Volunteer-Schemes/Victim-Care-Cadre-Programme
85	Roy, A., & Mukherjee, S. (2025). ShieldUp!: Inoculating Users Against Online Scams Using A Game Based Intervention. https://doi.org/10.48550/arXiv.2503.12341
86	Ibid.
87	Tech For Good Institute. (2025, April 14).

TECH FOR
GOOD
INSTITUTE