

Combating Scam Syndicates in Malaysia and Southeast Asia

By Dr Beh May Ting (Programme Coordinator & Senior Analyst, History & Regional Studies Programme)

Executive Summary

- Scams pose a major security and economic threat in Malaysia and the broader Southeast Asian region.
- These activities range from online scams to organized transnational syndicates that exploit digital vulnerabilities and regulatory gaps.

Malaysia lost RM54.02 billion, or equivalent to 3% of the nation's GDP to scams in 2024.

- As ASEAN Chair, Malaysia is prioritizing the curbing of job scam syndicates operating across Southeast Asia.
- Key policies to consider include strengthening cross-border cooperation, implementing robust legal frameworks, and leveraging technological innovations to combat scams effectively.

Combating Scam Syndicates in Malaysia and Southeast Asia

By *Dr Beh May Ting* (Programme Coordinator & Senior Analyst, History & Regional Studies Programme)

Introduction

The rise of digital finance, e-commerce, and online transactions has created new opportunities for fraudsters. From investment scams and phishing schemes to job fraud and love scams, these illicit activities cause financial losses amounting to billions of Ringgit annually. Many scam operations in Southeast Asia involve sophisticated cross-border syndicates; this makes enforcement challenging.

This paper examines the landscape of scams in Malaysia focusing on the most commonly reported ones, analyzes the regional scam ecosystem, and proposes policies to enhance prevention, enforcement, and public awareness. It emphasizes the need for cross-border cooperation, robust legal measures, and technological innovations in curbing the rising threat.

The Landscape of Scams in Malaysia

Scams continue to inflict severe financial and emotional distress in Malaysia, with the State of Scam Report 2024 revealing losses of RM54.02 billion (US\$12.8 billion), equivalent to 3% of the nation's GDP. Despite the staggering figures, 70% of victims did not report the scams, reflecting widespread skepticism toward the process. AI-driven scams such as deepfake videos and voice imitation are on the rise, with 25% of Malaysians unsure whether AI played a role in the scams they encountered. Additionally, 74% of respondents reported facing scams monthly, primarily through phone calls, messaging apps, and social media (Zainul, 2024). The average financial loss per victim stands at USD2,726, with only 2% managing to recover their funds. Investment scams remain the most prevalent (23%), followed by identity theft (21%) and shopping scams (20%) (Shahrizal, 2024). Malaysia also saw a sharp rise in scam calls, reaching US\$2.98 million last year; an 82.81% increase from US\$1.63 million in 2023, according to the 2024 Whoscall Annual Report (Fam, 2025).

In 2023, online crime cases reported to the Royal Malaysia Police surged by 35.5%, totaling 34,532 cases compared to 25,479 the previous year. E-commerce crimes accounted for the largest share at 33.2%, followed by telecommunications fraud (30.0%), non-existent investments (15.6%), fraudulent loans (12.3%), e-finance fraud (6.1%), and love scams (2.7%) (DOSM, 2024).

Table 1: Statistics of cases and losses for online crime by categories, Malaysia, 2021–2023.

Year	Total		Telecommunications crime		e-Finance		Love scam		e-Commerce		Non-existent loans		Non-existent investments	
	Cases	RM million	Cases	RM million	Cases	RM million	Cases	RM million	Cases	RM million	Cases	RM million	Cases	RM million
2021	26,257	698.44	6,423	199.56	896	73.45	1,460	56.74	9,499	73.03	4,784	50.60	3,195	245.06
2022	25,279	851.12	7,732	321.36	1,257	76.22	792	56.27	9,258	139.99	3,174	37.45	3,266	219.84
2023	34,532	1,220.30	10,368	353.59	2,092	104.90	935	43.95	11,481	204.26	4,263	40.76	5,393	472.83

Source: Department of Statistics Malaysia, 2024

Online Scams

Online scams are evolving rapidly, using digital platforms to deceive users through phishing, fake e-commerce sites, and digital payment fraud. Phishing schemes trick victims into revealing sensitive information such as passwords and credit card details, by impersonating trusted institutions via emails or fraudulent websites. According to Cyber Security Malaysia (CSM), these attacks are increasingly localized, often mimicking government initiatives, major e-commerce platforms, and financial institutions. A growing concern is “smishing” (SMS-based phishing), where scammers pose as banks, high courts, e-wallet providers, employment websites, and delivery services like J&T and Pos Malaysia to steal personal data (The Malaysian Reserve, 2025).

In 2024 alone, the Royal Malaysia Police’s Commercial Crime Investigation Department recorded 35,368 scam cases, resulting in RM1.6 billion in financial losses—accounting for 84.5% of all commercial crimes reported during the year (Bernama, 2025a). Telekom Malaysia (TM) released an official statement warning customers about scam emails falsely informing them of cash prizes from a programme called “Bonus Hadiah Keluarga TM.” These emails attempt to deceive recipients into

providing personal details to claim a non-existent reward. Likewise, the Employees Provident Fund (EPF) has been cautioning members about fraudulent messages impersonating authorities, falsely offering early EPF withdrawals.

Fake e-commerce platforms attract victims with enticing deals which either fail to deliver goods or which steal payment details. Digital payment fraud, including unauthorized transactions and account takeovers, targets users of banking apps and e-wallets. With scammers increasingly using AI-generated impersonations and other advanced tactics, it has become essential that public awareness, cybersecurity defenses, and regulatory enforcement are strengthened.

Investment Scams

Investment scams prey on individuals seeking high returns, using deceptive tactics like Ponzi schemes, fake cryptocurrency investments, and illegal money-lending. Ponzi schemes promise lucrative profits but rely on funds from new investors to pay earlier ones, eventually collapsing when recruitment slows. Fake cryptocurrency investments exploit the hype around digital assets, enticing victims with fraudulent platforms, pump-and-dump schemes, or non-existent tokens. Illegal money-lenders, often operating under the guise of quick loans, impose exorbitant interest rates and use intimidation tactics to trap borrowers in a cycle of debt. To avoid these scams, individuals should verify investment opportunities, be wary of unrealistic returns, and consult licensed financial authorities before committing funds.

The Securities Commission Malaysia (SC) has identified social media platforms such as Facebook and messaging apps like Telegram as primary channels for scammers. A notable shift in 2023 saw fraudsters increasingly using e-wallets and cryptocurrency instead of traditional mule bank accounts (The Star, 2024a). By the third quarter of 2024 (3Q 2024), the SC had received 3,380 complaints and inquiries related to scams and unlicensed activities, marking a 28% rise from the previous year (The Star, 2024b). Investment scams in Malaysia are so prevalent that new cases continue to emerge frequently. At the time of writing, the incident most recently reported involved a medical officer who lost RM86,000 to a cryptocurrency scam (Bernama, 2025a).

Love Scams

Love scams have become a major concern in Malaysia, with fraudsters preying on victims' emotions to manipulate them into transferring money. Scammers often create fake identities on dating apps, social media platforms, or messaging services, pretending to be wealthy professionals, military personnel, or foreigners seeking companionship. Once trust is established, they fabricate emergencies or investment opportunities to solicit funds. The Royal Malaysia Police reports that love scams accounted for 2.7% of all online fraud cases in 2023, with victims often left emotionally and financially devastated. Authorities continue to warn the public about these scams, urging vigilance when forming online relationships.

Among the noteworthy cases is a 2021 incident which involved a 63-year-old Malaysian widow who lost nearly RM3.9 million to a scammer she believed was a Korean businessman (Liew, 2022). Similarly, in one of the longest-running love scams reported, a 67-year-old woman lost more than RM2 million through 306 bank transfers into 50 different accounts over seven years to a scammer she met on Facebook, who posed as an American businessman working in medical equipment procurement in Singapore. Throughout their online "relationship," they never met in person, and the scammer fabricated various emergencies to solicit funds from her. (SCMP, 2024).

National Scam Response Center (NSRC)

The National Scam Response Center (NSRC) is a vital initiative in Malaysia's fight against financial scams; it provides a centralized and rapid response mechanism to detect, report, and mitigate fraudulent activities. Established as a collaborative effort between key agencies including the Royal Malaysia Police (PDRM), Bank Negara Malaysia (BNM), the Malaysian Communications and Multimedia Commission (MCMC), and financial institutions, the NSRC enhances coordination between law enforcement and the private sector. This inter-agency approach ensures a faster and more effective response to scams, thus reducing financial losses and increasing the chances of fund recovery (Prime Minister Department, 2024).

One of the NSRC's key functions involves its emergency response hotline (997), which allows victims to report scams in real-time (Teoh, 2022). This enables authorities to freeze fraudulent transactions, block scam-related bank accounts, and trace stolen funds before they are laundered or moved offshore. By providing immediate intervention, the NSRC minimizes the financial impact of scams and disrupts syndicate operations.

The NSRC also plays a crucial role in public awareness and prevention efforts. It collects and analyzes scam data to identify emerging fraud trends, which helps in developing proactive measures, including scam alerts, financial literacy programs, and policy recommendations (Camoens, 2023).

Scam Syndicates in Southeast Asia

Job scams have emerged as a major global concern, often leading to human trafficking and forced labour. Scammers attract victims with fraudulent job offers, promising lucrative salaries and attractive benefits abroad. However, upon accepting these offers, victims are trafficked to scam centres in countries such as Cambodia, Myanmar and Laos, where they are subjected to inhumane working conditions and constant threats of violence. Many are forced to engage in online scams, including cryptocurrency fraud and romance scams, under strict surveillance. Reports indicate that thousands, including Malaysians, have fallen victim to these syndicates. These syndicates thrive in countries with weak law enforcement, exploiting human trafficking as a recruitment strategy for their illicit

operations. In response, governments and law enforcement agencies across Southeast Asia are intensifying efforts to dismantle these networks, rescue victims, and educate the public on deceptive job offers.

As the 2025 ASEAN Chair, Malaysia is prioritizing efforts to combat job scam syndicates across Southeast Asia. ASEAN countries are enhancing cooperation through ASEANAPOL to tackle these syndicates, with previous discussions held in Labuan Bajo, Indonesia, and Vientiane, Laos. A recent example of regional collaboration is Myanmar handing over 320 foreign nationals, including Malaysians, who were victims of job scams. These individuals were transferred to Thailand's National Referral Mechanism for identity verification before repatriation (The Star, 2025).

In a separate case, The Ministry of Foreign Affairs (Wisma Putra) confirmed the rescue of 60 Malaysian nationals believed to be victims of a transnational job scam syndicate. The operation, carried out by Cambodian authorities on February 22, targeted illicit online scam compounds in Poipet, a region near the Cambodia-Thailand border. Following the rescue, the victims were transferred to an immigration detention centre in Siem Reap for identity verification and further processing (Bernama, 2025b).

Malaysia has been actively enhancing its diplomatic and law enforcement strategies to combat the escalating issue of scam syndicates. In collaboration with international partners, Malaysia participated in Operation First Light 2024, a global initiative targeting online scammers. This operation, involving 61 countries, led to the arrest of approximately 3,950 suspects and the seizure of \$257 million in illicit assets. The operation also facilitated the freezing of 6,745 bank accounts associated with fraudulent activities (INTERPOL, 2024). Through these concerted efforts, Malaysia aims to strengthen its position in leading both diplomatic and law enforcement initiatives to mitigate the growing problem of scam syndicates.

Limitations in Existing Legal Frameworks

One of the key challenges in combating scam syndicates is the inadequacy of existing legal frameworks which often struggle to keep pace with evolving cyber threats. Many countries rely on outdated cybercrime laws that do not fully address emerging digital fraud tactics, such as AI-powered scams, deepfake impersonations, and cryptocurrency-based money laundering. While laws like Malaysia's Computer Crimes Act 1997 and the Personal Data Protection Act 2010 provide a foundation for cybersecurity enforcement, they lack provisions for tackling sophisticated online fraud and cross-border cybercrime networks.

Furthermore, weak enforcement of anti-money laundering regulations hampers efforts to dismantle scam syndicates. Despite the presence of anti-money laundering laws, loopholes in financial oversight allow fraudsters to exploit offshore accounts, cryptocurrency transactions, and shell companies to launder illicit funds. The lack of real-time monitoring mechanisms and cooperation between financial

institutions and law enforcement agencies makes it difficult to track and freeze scam-related assets before they are funneled out of the country.

Another major limitation is the jurisdictional challenge posed by international scam networks. Many syndicates operate from countries with weak regulatory enforcement, which makes extradition and prosecution difficult. Scam operators based in Cambodia, Myanmar, and Laos, for example, often target victims across Southeast Asia while evading local law enforcement. Limited bilateral agreements and delays in cross-border legal cooperation hinder efforts to apprehend perpetrators and recover stolen funds. Addressing these challenges requires comprehensive legal reforms, stronger international cooperation, and enhanced regulatory mechanisms to close loopholes exploited by scam syndicates.

Challenges in Enforcement

A significant challenge is the prosecution of transnational scam syndicates which operate across multiple jurisdictions with varying levels of legal enforcement. Many scam hubs are based in countries with varying regulatory oversight, such as Cambodia, Myanmar, and Laos, making it difficult for Malaysian authorities to apprehend perpetrators or recover stolen assets. Limited extradition agreements and slow cross-border legal cooperation further complicate efforts to dismantle these networks. Even when scammers are caught, gaps in evidence gathering and the reliance on outdated cybercrime laws make it difficult to secure convictions.

Additionally, enforcement agencies often lack advanced technological tools to effectively track and combat digital fraud. Scammers use sophisticated techniques such as end-to-end encrypted messaging, AI-generated deepfake identities, cryptocurrency laundering, and multi-layered proxy servers to evade detection. Without robust real-time surveillance systems, AI-powered fraud detection, and better forensic capabilities, law enforcement struggles to keep pace with evolving cyber threats. Addressing these challenges requires a more integrated enforcement strategy, stronger regional collaboration, and greater investment in next-generation cybersecurity technologies.

Policy Recommendations

To effectively address the rising threat of scam syndicates, a multi-pronged, data-driven approach is necessary, which combines legislative reforms, cross-border cooperation, technological advancements, financial regulations, and public awareness initiatives.

1. Strengthening Legal Frameworks

- *Modernizing Cybercrime Laws*

Malaysia's Computer Crimes Act 1997 and Communications and Multimedia Act 1998 are outdated; it lacks provisions for AI scams, deepfake fraud, and crypto crimes. Challenges remain in integrating

advanced detection systems and improving cross-border cooperation. To combat evolving threats, Malaysia must introduce stricter penalties and update legal frameworks for online fraud. Additionally, collaborating with IT specialists and cybersecurity experts is crucial in formulating tech-driven policies that address evolving digital threats and enhance enforcement capabilities.

- *Expanding Anti-Money Laundering (AML) Regulations*

Malaysia's Anti-Money Laundering, Anti-Terrorism Financing & Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA) remains the cornerstone of AML legislation, but evolving financial scams demand stronger measures. With scams increasingly exploiting crypto wallets, offshore accounts, and mule accounts, Malaysia has made strides in AML enforcement, including integrating fintech through the Financial Technology Regulatory Sandbox Framework by Bank Negara Malaysia. In order to enhance financial security, AML laws should mandate real-time transaction monitoring, enforce strict verification for cryptocurrency exchanges, and impose stricter reporting obligations on fintech platforms.

2. Enhancing Cross-Border Law Enforcement & Intelligence Sharing

- *Strengthening ASEAN-Wide Law Enforcement Coordination*

The ASEAN Cybercrime Task Force, which was mooted earlier this year, should integrate law enforcement agencies from Malaysia, Singapore, Thailand, Cambodia, Myanmar, and China for joint operations against syndicates operating in scam hubs across Southeast Asia. Malaysia should also accelerate the ratification of bilateral extradition agreements and mutual legal assistance treaties with countries harbouring scam syndicates.

- *Deploying Cyber-Liaison Officers*

Malaysia can deploy cybercrime specialists to its embassies in high-risk countries such as Cambodia, Laos, and Myanmar, where scam syndicates are known to operate. These specialists would serve as liaison officers, working closely with local law enforcement agencies to enhance intelligence-sharing, expedite investigations, and facilitate cross-border cooperation in tackling cybercrime. By embedding cybercrime experts within embassies, Malaysia can proactively monitor scam networks, provide real-time support to affected citizens, and bolster regional cybersecurity efforts through direct engagement with ASEAN counterparts.

3. Leveraging Technology to Combat Scams

- *National AI-Powered Fraud Detection System*

Malaysia should implement a real-time fraud analytics platform linking banks, telcos, e-wallets, and enforcement agencies to detect and block fraudulent transactions instantly. Additionally, Malaysia should implement mandatory biometric authentication for all high-value online banking, fintech, and crypto transactions.

- *Blocking Fraudulent Numbers & Accounts in Real-Time*

Malaysia should establish a National Scam Intelligence Database to centralize and streamline efforts in combating financial fraud and cyber scams. This database should be designed to detect, track, and

block phone numbers, bank accounts, and cryptocurrency wallets linked to scam syndicates in real-time.

4. Public Awareness & Digital Literacy Campaigns

- *National Anti-Scam Education Programme*

To equip young Malaysians with the knowledge to identify and avoid scams, scam awareness training should be formally incorporated into school curriculums starting from primary education. The Ministry of Education should collaborate with cybersecurity experts, financial institutions, and law enforcement agencies to develop engaging, age-appropriate modules on common scams, such as phishing, fake job offers, investment fraud, and social media scams.

- *Large-Scale, Multilingual Public Awareness Campaigns*

A nationwide scam awareness campaign should be launched across multiple platforms, to ensure that information reaches people of all ages and backgrounds. Social media collaborations with influencers and content creators on platforms like Facebook, TikTok, YouTube, and Instagram can make scam awareness more engaging and accessible in multiple languages. Additionally, government agencies, NGOs, and local authorities should conduct workshops, town halls, and roadshows in both urban and rural areas to strengthen public awareness and fraud prevention efforts.

- *Scam Simulation & Training for Businesses*

Companies should conduct regular scam simulation exercises to train employees in detecting fraud, especially in banking, telecommunications, and e-commerce. These exercises should mimic real scam tactics, incorporate AI-driven detection tools, and reinforce clear reporting mechanisms. Strengthening fraud awareness helps protect customer data and minimize financial losses.

References

- Bernama. (2025a, March 5). Medical officer loses over RM86,000 to Cryptocurrency Scam. Available at https://www.bernama.com/en/crime_courts/news.php?id=2399047
- Bernama (2025b, February 26). 60 Malaysians rescued from job scam syndicate in Cambodia, says Wisma Putra. Free Malaysia Today. Available at <https://www.freemalaysiatoday.com/category/nation/2025/02/26/60-malaysians-rescued-from-job-scam-syndicate-in-cambodia-says-wisma-putra/>
- Camoens, A. (2023, November 21). National scam hotline in overdrive. The Star. Available at <https://www.thestar.com.my/news/nation/2023/11/21/national-scam-helpline-in-overdrive>
- Department of Statistics Malaysia (DOSM). 2024, October 16. Crime Statistics, Malaysia, 2024. Available at <https://www.dosm.gov.my/portal-main/release-content/crime-statistics-malaysia->
- Fam, C. (2025, March 3). Report: Scam calls in Malaysia skyrocketed by 82.81% in 2024. The Star. Available at <https://www.thestar.com.my/tech/tech-news/2025/03/03/report-scam-calls-in-malaysia-skyrocketed-by-8281-in-2024>
- INTERPOL. (2024, June 27). USD 257 million seized in global police crackdown against online scams. Available at <https://www.interpol.int/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams>
- Liew, J.X. (2022, March 21). Widow loses almost RM3.9mil in love scam. The Star. Available at <https://www.thestar.com.my/news/nation/2022/03/21/widow-loses-almost-rm39mil-in-love-scam>
- Prime Minister Department. (2024, July 3). About NSRC. National Anti-Financial Crime Centre. Available at <https://nfcc.jpm.gov.my/index.php/en/component/content/article/about-nsrc?catid=17&Itemid=114#:~:text=As%20announced%20by%20the%20Prime%20Minister%27s%20Department%20on,to%20coordinate%20rapid%20response%20to%20online%20financial%20fraud.>
- Shahrizal. (2024, October 4). Malaysia Loses RM54.02 Billion To Scams, Report Reveals Alarming Rise. Business Today. Available at <https://www.businesstoday.com.my/2024/10/04/malaysia-loses-rm54-02-billion-to-scams-report-reveals-alarming-rise/#:~:text=The%20State%20of%20Scam%20Report%202024%2C%20conducted%20by,key%20insights%20into%20the%20country%E2%80%99s%20fight%20against%20scams.>
- South China Morning Post (SCMP). (2024, December 18). 7-year love scam costs Malaysian woman nearly US\$500,000. Available at <https://www.scmp.com/news/asia/southeast-asia/article/3291304/7-year-love-scam-costs-malaysian-woman-nearly-us500000>
- Teoh, P.Y. (2022, October 14). Call NSRC at 997 to report online financial scams. New Straits Times. Available at <https://www.nst.com.my/news/crime-courts/2022/10/840462/call-nsrc-997-report-online-financial-scams>
- The Malaysian Reserve. (2025, January 23). The mounting landscape of phishing scams. Available at https://themalaysianreserve.com/2025/01/23/the-mounting-landscape-of-phishing-scams-in-malaysia/?utm_source=chatgpt.com
- The Star. (2024a, November 7). Scam complaints in Malaysia up 300% since 2019. Available at <http>

s://www.thestar.com.my/news/nation/2024/11/07/scam-complaints-in-malaysia-up-300-since-2019

The Star. (2024b, October 11). SC records 3,380 complaints on scams, unlicensed activities as of 3Q24. Available at <https://www.thestar.com.my/business/business-news/2024/10/11/sc-records-3380-complaints-on-scams-unlicensed-activities-as-of-3q24>

The Star. (2025, February 17). Job scam issue among Malaysia's priorities as Asean chair, says Deputy Foreign Minister. Available at <https://www.thestar.com.my/news/nation/2025/02/17/job-scam-issue-among-malysias-priorities-as-asean-chair-says-deputy-foreign-minister>

Zainul, E. (2024, October 3). Malaysians lost US\$12.8b to scams over the past year, survey reveals. The Edge Malaysia. Available at <https://theedgemaalaysia.com/node/728964>

Managing Editor:
Ooi Kee Beng

Editorial Team:
Tan Lee Ooi and Nur Fitriah (designer)

PENANG
INSTITUTE
making ideas work

10 Brown Road
10350 George Town
Penang, Malaysia

Tel : (604) 228 3306
Web : penanginstitute.org
Email : issues@penanginstitute.org

© Copyright is held by the author or authors of each article.

The responsibility for facts and opinions in this publication rests exclusively with the authors and their interpretations do not necessarily reflect the views or policy of the publisher or its supporters.

No part of this publication may be reproduced in any form without permission.