KHAZANAH RESEARCH INSTITUTE

DISCUSSION PAPER 05/26 | 28 AUGUST 2026

Hook, Line and Sinker: Cyber Financial Scams in Malaysia

Jun-E Tan, Bor Neng Quan and Kuhaneetha Bai Kalaicelvan

Khazanah Research Institute

The **KRI Discussion Papers** are a series of research documents by the author(s) discussing and examining pressing and emerging issues. They are stand-alone products published to stimulate discussion and contribute to public discourse. In that respect, readers are encouraged to submit their comments directly to the authors.

The views and opinions expressed are those of the author and may not necessarily represent the official views of KRI. All errors remain authors' own.

DISCUSSION PAPER 05/26 | 28 AUGUST 2026

Hook, Line and Sinker: Cyber Financial Scams in Malaysia

This discussion paper was prepared by Dr. Jun-E Tan (Senior Research Associate), Bor Neng Quan (Consultant Research Associate) and Kuhaneetha Bai Kalaicelvan (Former Research Intern) from the Khazanah Research Institute (KRI).

The authors are grateful for valuable comments from Dr. Anya Schiffrin (Technology Policy and Innovation (TPI) Concentration at Columbia University), Ts. Dr. Mohamad Nizam bin Kassim (National Anti-Financial Crime Centre), Navya Sinha (Columbia University), Dr. Rachel Gong (KRI) and Salbiah Idris (KRI).

Authors' email address: **june.tan@krinstitute.org & consultant.nengquan@krinstitute.org**

Published 28 August 2026. Published by Khazanah Research Institute at Level 17-1, Mercu UEM, Jalan Stesen Sentral 5, Kuala Lumpur Sentral 50470 Kuala Lumpur, Malaysia. Tel: +603 2705 6100; Fax: +603 2034 0000; Email: enquiries@KRInstitute.org

Cover photo by weerapatkiatdumrong | iStock

ABBREVIATIONS

AML	:	Anti-Money Laundering
AMLATFPUAA	:	Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act
ASP (C) License	:	Application Service Provider Class License
ASPs	:	Application Service Providers
AI	:	Artificial Intelligence
ATM	:	Automated Teller Machine
BNM	:	Central Bank of Malaysia
CSO	:	Civil Society Organization
CCID	:	Commercial Crime Investigation Department
CMA	:	Communications and Multimedia Act
SSM	:	Companies Commission of Malaysia
CCA	:	Computer Crimes Act
CASPs	:	Content Application Service Providers
CFT	:	Countering Financing of Terrorism
CSA	:	Cyber Security Act
CyberSAFE®	:	Cyber Security Awareness for Everyone
CSM	:	Cybersecurity Malaysia
DEXs	:	Decentralised Exchanges
DOSM	:	Department Of Statistics Malaysia
DAXs	:	Digital Asset Exchanges
FOMCA	:	Federation Of Malaysian Consumers Associations
FTAF	:	Financial Action Task Force
FSA	:	Financial Services Act
LHDN	:	Inland Revenue Board of Malaysia
ISPs	:	Internet Service Providers
IFSA	:	Islamic Financial Services Act
KSSR/KSSM	:	Kurikulum Standard Sekolah Rendah/Menengah
MCCA	:	Malaysia Cyber Consumer Association
MACC	:	Malaysian Anti-Corruption Commission
MCMC	:	Malaysian Communications and Multimedia Commission
KD	:	Ministry Of Digital
KPDN	:	Ministry Of Domestic Trade and Cost of Living
MoE	:	Ministry Of Education

MoHE	:	Ministry Of Higher Education
MASSA	:	Mobile Assessment Security Scanning Application
MTO	:	Money Transfer Operators
MIMO	:	Multi-Input-Multi-Output
NAD	:	National Addressing Database
NFCC	:	National Anti-Financial Crime Centre
NCII	:	National Critical Information Infrastructure
NACSA	:	National Cyber Security Agency
NFIS	:	National Financial Crime Intelligence System
NFP	:	National Fraud Portal
NICTSeD	:	National ICT Security Discourse
NLP	:	National Language Processing
NRIC	:	National Registration Identity Card
NSRC	:	National Scam Response Centre
OTP	:	One Time Password
ODR	:	Online Dispute Resolution
ONSA	:	Online Safety Act
PDPA	:	Personal Data Protection Act
PINs	:	Personal Identification Numbers
PETs	:	Privacy Enhanced Technologies
PDRM	:	Royal Malaysia Police
SC	:	Securities Commission
SRF	:	Shared Responsibility Framework
SMS	:	Short Message Service
JPDP	:	Personal Data Protection Department
URL	:	Uniform Resource Locator
UNICEF	:	United Nations Children's Fund
UNDP	:	United Nations Development Programme
VPN	:	Virtual Private Network

DISCUSSION PAPER 05/26 | 28 AUGUST 2026

Hook, Line and Sinker: Cyber Financial Scams in Malaysia

Jun-E Tan, Bor Neng Quan and Kuhaneetha Bai Kalaicelvan

Summary

In 2025, the Home Ministry reported that online scams caused RM2.77 billion in losses, translating to roughly RM7.6 million lost daily[1]. Cyber financial scams have emerged as a significant threat as Malaysians spend more time online and increase their use of digital financial services. This trend shows no signs of abating as scammers get increasingly sophisticated, using technology to scale up their operations and refine their deceptive tactics.

In this paper, we define cyber financial scam as "financial loss caused by a victim's voluntary actions as a result of trickery performed by the perpetrators in an online space".

This study dives into the problem of cyber financial scams in the Malaysian context to glean insights into key issues using a systemic perspective. The research objectives are as follows:

1. To understand the anatomy of a cyber financial scam, focusing on the chain of events that occur and their underlying issues;
2. To identify gaps within Malaysia's existing regulatory and non-regulatory initiatives on the problem; and
3. To propose policy recommendations to improve the work around combatting scams.

Using desk research and drawing from stakeholder discussions, we developed a Scam Anatomy framework that outlines the key stages within a typical scam lifecycle from the perspective of the scammers. We find that scams usually move through seven stages, from the initial groundwork and operational setup, to the establishment of contact and interactions with the victim, to the final disappearing act and cashing out of extracted funds.

With the framework thus established, we used it to analyse Malaysia's current regulatory and non-regulatory initiatives to combat scams. From our mapping, we observe that a plethora of regulations already exist across the scam lifecycle, with most gaps in the governance of technological advancements even though the government is moving rapidly on closing these gaps. While much effort has been poured into mitigation and safeguards, initiatives tend to be reactive,

[1] FMT (2026a)

focusing on the financial extraction end of the scam lifecycle. There is also disproportionate focus on literacy campaigns and individual responsibility.

To tackle cyber financial scams and scam outcomes more effectively, we recommend the following priorities:

- **To distribute risk and responsibility among key enabling actors,** rather than placing the full burden on individuals when scams occur. This approach ensures that institutional actors, such as financial institutions, telecommunication companies, and application service providers are held accountable for effectively discharging their obligations in preventing and addressing scams.
- **To develop technological solutions to connect and build upon existing legal and information systems** to match the speed and scale of malicious actors. For example, a scam advertisement detection tool can be used together with legal provisions from the Online Safety Act for effective content takedowns. A dedicated scam prevention app integrating existing official databases and tools can also serve as a single source of truth of verification and response guidance for consumers.
- **To provide accurate, timely and publicly available data for scam monitoring** by having a public-facing dashboard. Such a dashboard can reduce cross-agency data discrepancies, provide a transparent baseline for comparison along with valuable indicators, and thereby increase public vigilance and improve incident reporting rates.
- **To enhance literacy campaigns to build anti-scam resilience** by moving beyond basic information on scam identification towards more engaging, innovative, and evidence-based approaches. Likewise, simulation training and scam-awareness sandboxes should be considered as part of broader efforts to build a scam-resilient population.
- **To close legal gaps and enact forward-looking legislation,** particularly on areas related to emerging technology. Legislations should adopt a preventive rather than reactive approach to better respond to emerging threats.
- **To increase law enforcement capacity and safeguards** – more resources should be invested to keep pace with the growing sophistication of scams, while appropriate safeguards are put in place to address unintended effects of tight enforcement.
- **To strengthen cybersecurity defence** by investing in, nurturing and developing more cybersecurity talent.

Table of Contents

1. Introduction

1.1. Background

Scams have long been a persistent problem in Malaysia and continue to grow rapidly, exacerbated by technological advancements.

Most scam cases today happen online. According to Commercial Crime Investigation Department (CCID) of Polis Diraja Malaysia (PDRM), online elements are involved in approximately 90% of commercial crime cases currently under investigation[2]. In 2025, the Home Ministry reported a staggering RM2.77 billion in losses resulting from online scams in that year alone. This translates to roughly RM7.6 million lost to online scams every single day[3].

Behind every number and statistic lies a devastating story: hard-earned money is lost, trust is broken, and relationships are damaged. At the national level, scams pose serious threats to economic stability, public safety and digital trust. Private entities such as telecommunications companies, financial institutions, and other service providers have to dedicate resources to combat the issue, or lose consumer trust when high profile cases happen. Tackling scams is therefore not a problem only for the individual, a singular institution or the government; it is a shared responsibility. Addressing the situation requires a whole-of-nation approach.

A review of academic literature finds that most studies on the topic of online scams in Malaysia tend to focus on narrow aspects such as techniques used by particular scams, without considering the problem holistically from a lifecycle and systemic perspective. There is limited research that systematically breaks down problems associated with cyber financial scams, in analysing the chain of events from the targeting of victims in online spaces to the eventual financial extraction, to inform a more targeted approach to addressing the issues.

1.2. Research Questions

As such, this study intends to:

1. Understand the anatomy or structure of a cyber financial scam, focusing on the chain of events that occur and underlying issues that enable them;
2. Identify and analyse the existing gaps within Malaysia's regulatory and non-regulatory frameworks on the problem; and
3. Propose recommendations for Malaysian stakeholders to address the growing threat of cyber financial scams.

[2] FMT (2026b)
[3] FMT (2026a)

1.3. Significance and Structure of the Paper

There are three main contributions of this paper, each covered in an individual section.

The first (in Section 2) is a Scam Anatomy that outlines the end-to-end scam lifecycle, describing the typical modus operandi at each stage. This enables the regular reader to establish a clear understanding of steps involved in a scam from the perpetrator's perspective.

The second (in Section 3) is a comprehensive mapping of regulatory and non-regulatory initiatives in Malaysia, organised by core issues of each stage of the Scam Anatomy. Relevant stakeholders are highlighted per stage, and we suggest gaps that can be filled. This section will be useful for researchers, policymakers and readers who are seeking details in Malaysia's context.

The third (in Section 4) is a set of policy recommendations that we have compiled for relevant stakeholders to consider and implement. We draw from other countries such as Singapore, Taiwan and Australia to illustrate approaches that may be useful in the context of Malaysia.

1.4. Methodology and Approach

This study draws from desk research and expert insights from a roundtable discussion, "Best Practices for Regulatory Approaches to AI-Deepfakes Used in Financial Scams", co-organised by Khazanah Research Institute and Columbia University in the City of New York, in Kuala Lumpur on 20 November 2025. The Roundtable involved 23 Malaysian and international stakeholders from the United States, Indonesia, Australia, Singapore and Taiwan (see full list in Appendix 1). The participants represented diverse perspectives from policymakers, academics, industry players, civil society organisations, lawyers and law enforcement.

We also had follow-up interviews with three local participants after the roundtable to obtain further information and corroborate our findings with the stakeholders' experiences on the ground.

2. Setting the Scene

2.1. Typology of Scam, Fraud and Crime

In the financial context, terms such as cyber scam, cyber fraud and cyber crime are often used interchangeably[4]. All are harmful acts happening within the online space that result in monetary loss. We start by making distinctions among the three to set the foundation of the paper.

Table 1 shows the typology of 'scam', 'fraud' and 'crime'. The key difference between "scam" and "fraud" lies in the deception that induces voluntary action from the victim. In scams, victims themselves are persuaded to transfer funds to the perpetrators, whereas in frauds, the perpetrators run covert operations to obtain the funds directly. "Crime" refers to the offences in the legal context[5].

The focus of this paper is **cyber financial scams,** i.e. financial loss caused by a victim's voluntary actions as a result of trickery performed by the perpetrators in an online space.

Table 1: Typology of 'scam', 'fraud' and 'crime'

	Cyber Financial Scam	Cyber Financial Fraud	Cyber Financial Crime
Definition	Financial loss caused by a **victim's voluntary actions** as a result of trickery performed by the perpetrators in an online space.	Financial loss caused by **unauthorised activity** in an online space on the victim's behgo that is conducted without their awareness.	Any illegal acts committed in an online space for financial gain that violate the law and are deemed punishable offences, including but not limited to cyber financial scams or fraud.

Source: Arthur State Bank (n.d.), Mastercard (n.d.), HSBC UK (n.d.), Ambashtha and Kumar (2023); EUROPOL (n.d.)

2.2. Anatomy of a Cyber Financial Scam

Scams are not new; they have manifested in varied forms and have been executed via different methods throughout time. As technologies advance, scams have evolved to become more complex and widespread, but still retain similar characteristics and goals. To better understand how cyber financial scam processes work, we have drawn from established scam frameworks to produce a cyber financial scam anatomy (hereinafter referred to as the Scam Anatomy) that is fit for purpose in a cyber environment.

Edward H. Smith's 1922 Confidence Trick Strategy[6] and David W. Maurer's 1940 The Big Con[7] are foundational reference points for understanding the basics of a scam, being two of the earliest

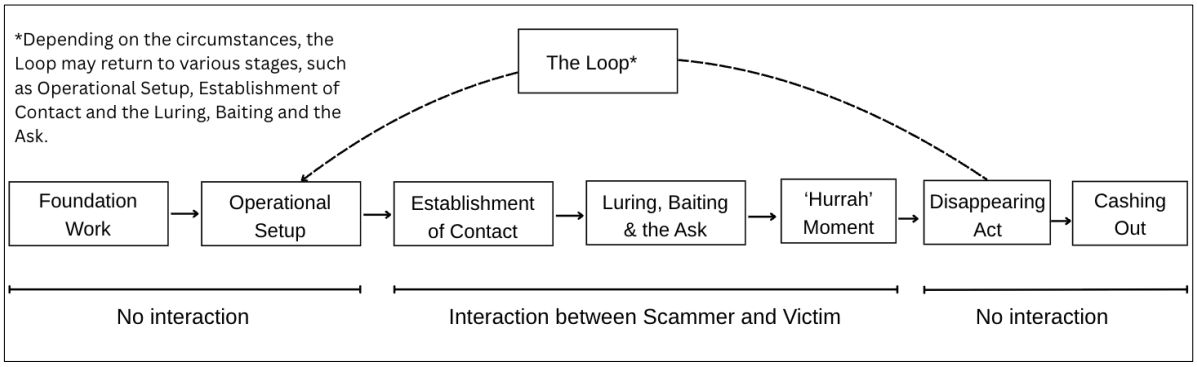
[4] Tech For Good Institute (2025)
[5] Kaspersky (2019)
[6] Estrella (2021)
[7] Maurer (2010)

scam frameworks that have stood the test of time. Both frameworks outline a similar start-to-end process. Scams begin with extensive preparation and planning, followed by efforts to build trust to deceive victims into handing over money, and conclude with a disappearance at the end.

The evolution of scam activities warrants a closer examination of more recent frameworks to account for the changing nature of scam operations. The United Nations Development Programme's (UNDP) Scam Journey Map[8], developed in 2025, is a more up-to-date framework to understand scams in the digital era. It highlights additional elements beyond the scam process that were later incorporated into our Scam Anatomy framework. This gives a more accurate and comprehensive depiction of the entire scam lifecycle.

Informed by the existing frameworks as discussed above, we have come up with a comprehensive Scam Anatomy that is applicable to most scam cases today. Every stage of the anatomy addresses different forms of activities undertaken by the perpetrators in conducting the scam. While the UNDP's scam framework provides a thorough visualisation to the end-to-end scam process, we have simplified and streamlined the whole process, anchoring it on the angle of the perpetrators. This allows a targeted focus on each stage of the scam activity in Section 3.

Figure 1: Cyber Financial Scam Anatomy



Source: Authors' visualisation

Drawing inspiration from the UNDP's Scam Journey Map, which covers both perspectives of the victim and the perpetrator, the stages of the Scam Anatomy are differentiated into either "no interaction" or "interaction between scammer and victim". This highlights the significant amount of behind-the-scenes work in executing a successful scam operation as well as the critical window in which the scammer comes into contact with the victim.

To clarify, a targeted individual transitions from a potential victim to an actual one when money changes hands – not all targets become victims. However, for simplicity in describing the process, the description that follows will refer to the role of the targeted individual as "victim".

[8] Hooper, Bannear, and Chew (2025)

Below, we go through each stage in detail to understand the process flow of a scam, which is a common structure that applies to most scams in all manner of variations; we also expand on cyber-enabled aspects where applicable.

Foundation work

In the early stages of a cyber financial scam, foundational work focuses on laying the groundwork to pull off a successful scam, mainly involving the thinking behind various aspects of the scam operation such as the timing, scalability, and potential countermeasures from the relevant authorities. According to Estrella (2021), this stage can be divided into three sub-phases.

Research: Background research is conducted to enable a deeper understanding of the targeted victims and the environment where the scam will take place. The findings guide the formulation of strategies in planning out the scam activities.

Strategy: Based on findings of the background research, a detailed and overarching strategy is designed by the masterminds. This is important to ensure consistency in executing the plan throughout the scam cycle to reduce the likelihood of failure, or being detected.

Obtain: Resources that are necessary to operationalise the scam activity are obtained at this stage. This includes the gathering of information or data about the potential victims and obtaining financial resources.

One of the main ways for scammers to obtain personal information of potential victims is through acquiring data leaked from data breaches of insecure government or company databases.

Operational setup

Also known as the "preparation" phase[9], this phase sets the stage for the scam activity. The type of preparation needed varies with the nature of the scam. For cyber financial scams, some of the preparatory work includes the setting up of fake profiles, content and even platforms, as discussed below.

Creation of fake profiles: Scammers use SIM cards to set up fake profiles and accounts. SIM cards, an important element for scam activity, are favoured by scammers because they are disposable and easily replaceable, affording anonymity when registration processes are lax. According to the Global Anti-Scam Organisation, one of the main criminal uses of SIM cards is for the creation of fake accounts, such as in the case of registering for major messaging apps like Telegram and WhatsApp that need an active mobile number for One Time Password (OTP). The same verification process applies to the registration of certain major email accounts (which is in turn needed to sign up for a social media account), bank accounts, crypto wallet, etc[10].

[9] Mouton et al. (2014)
[10] Global Anti-Scam Org (2025)

Generation of fake content: Scammers create content that would be used throughout the scam operations. For instance, scammers can now rely on AI-powered image generation tools to generate realistic pictures for their profiles. With AI, anyone with basic AI knowledge can create these contents with minimal cost. The same persona can be pictured in different settings, such as in a workplace, on vacation, and so on. By showcasing these photos on social media posts, the scammer increases the realness of the profile.

In later stages of the scam operation, modern generative AI tools can craft human-like messages that match the tone as desired by the scammers, such as text-based content that resembles a legitimate company, or personalised text messages targeting specific victims. In addition, highly realistic synthetic media (also known as deepfakes) can dupe victims by manipulating the likenesses of real people or manufacture events in pictures, video or audio.

Creation of fake platforms: One of the most common ways to trick victims into a spoofed website (a deceptive version of a real website) is through masked Uniform Resource Locator (URL). URL masking is a classic technique used by perpetrators to use a false but highly similar URL of the actual website[11]. If victims fail to identify the minor difference and click on the link, the spoofed URL will take them to a fake website that looks just like the actual website. Box 1 illustrates an interesting case study of the Semak Mule platform run by PDRM that was spoofed and used as a base for financial scams.

To make matters worse, scammers can now clone legitimate websites easily with the help of AI. According to the Wall Street Journal, through an AI-powered tool procured from a criminal marketplace or dark-web forum, perpetrators can clone a legitimate site just by inserting the URL of the desired site. Within a brief period of time, the tool can scrape the legitimate webpage and duplicate its appearance and design. The scammers can then tweak the fake webpage according to their liking, for instance, in adding forms to steal victims' financial or personal details[12].

Fake apps, just like fake websites, are designed by scammers to resemble legitimate software to gain the victim's trust. Victims will encounter these fake apps through different channels, with unofficial app stores or app galleries being the most common distribution point, alongside malicious ads, malicious links, or in some rare cases, the official app store[13].

[11] Consumer Protection Team (n.d.)
[12] Snow (2025)
[13] Chandraiah et al. (n.d.)

Box 1: Semak Mule platform spoofed and used for financial scams

Semak Mule Platform Spoofed and Used for Financial Scams

Semak Mule is a platform operated by PDRM's CCID to help users check if bank accounts, company names and phone numbers have been implicated in fraudulent activity before. It is usually a trusted source of information for victims in Malaysia.

However, the Online Safety IRL program run by Ratio:Cause, through their Instagram account, shared an incident on 4 February 2026 about the existence of a fake Semak Mule website[5]. This website was a duplicate of the original Semak Mule platform, and used a different top-level domain (TLD), *.com* instead of *.rmp.gov.my*.

The website directed visitors seeking to verify information to WhatsApp, where they were instructed to make "reports". Based on Ratio:Cause's recount of the incident, the scammer impersonated a PDRM officer and took details from the victim, pretending to generate a police report. The scammer then attempted to convince the target to send over money by promising them that they would be able to regain their stolen funds. When the victim mentioned that they had gone to an actual police station to file the report, the scammer ceased all communication and deleted the fake police report.

At the time of writing, the fake Semak Mule website using the *-.com* TLD has been taken down, but it goes to show that even the official mechanisms set in place to combat scams can become tools for scammers themselves.

Establishment of contact

This stage marks the first instance of contact between the perpetrators and the potential victims. Through interactions via various communication channels, with approaches that are direct or indirect, targeted or scattered – the perpetrators establish connections with the potential victims with the goal of scamming them.

Luring, baiting & the ask

By employing different tactics such as building deeper bonds, establishing trust or faking a sense of urgency, the perpetrators will engage in activities that seek to lure and bait the victims to gradually fall prey to the scams. When the time is ripe, the perpetrators will nudge the victims to perform certain activities ("the Ask") that will lead to financial loss for the victims. Social engineering (see Box 2) is a technique commonly used at this stage.

Box 2: Social engineering used in scams

Social Engineering in Scams

Unlike hacking which exploits technological vulnerabilities, social engineering's primary objective is psychological manipulation to "exploit human error"[14]. Victims are lured into performing actions that benefit the attacker, such as granting access to accounts, transferring money, or revealing sensitive information (e.g. card details). To psychologically manipulate individuals, scammers employ guilt, deception, blackmail, and flattery in their interactions[15].

Social engineering can be considered as an attack of its own in other cybercrimes. Within the context of scams, it is usually deployed in the Luring and Baiting stage as the scammer interacts with the victim to lead up to the Ask.

Social engineering messages depend on a range of factors to successfully manipulate the victim, targeting human's "natural behaviour, emotions and motivations" [16]. While scammers may control the narrative of the message itself, it is not the only factor that determines the susceptibility of victims towards manipulation. Victims could be more or less vulnerable towards false communications due to their lived experiences and dispositional factors[17].

'Hurrah' moment

The scammer successfully obtains funds from the victim. Depending on the type of scam, this could be of the victim's own volition in transferring funds after either positive or negative encouragement, or by gaining access to victims' finances. The distinction between positive and negative encouragement is determined by the type of emotion the action invokes. If the scammers' actions result in fear, panic, or stress, coercing the victim to transfer funds, this is considered as negative encouragement. On the flip side, if the scammer persuades the victim through emotions like enthusiasm, optimism and hope, this would be positive encouragement.

Disappearing act

Upon achieving the desired objectives, the scammer vanishes with the aim of leaving no trace behind. This happens with or without the victim's realisation. To remain undetectable, the

[14] Kaspersky (2020)
[15] Butts and Renee (2024)
[16] Marchand (2025)
[17] Norris, Brookes, and Dowell (2019)

scammer quickly removes all digital trails, forms of online presence and any available proof - redirecting leads and becoming uncontactable. While there are many methods used by online scammers to erase their trails, the methods can be generally categorised into three types usually associated with cyberattacks[18].

Obscurity: The perpetrator attempts to evade systemic triggers and alarms used for detection. By understanding detection methods and thresholds used by systems such as a bank's transaction monitoring mechanism, they are able to obfuscate their origins or manage activities to prevent triggers. Technical methods used to accomplish these include hiding the source and destination of network traffic such as using virtual private networks (VPNs) and TOR browsing[19].

Obliteration: Obliteration refers to a complete deletion of perpetrators' traces of activity. This includes deleting any chat, browser, site or system activity logs, fake user accounts used to execute the scam, and files associated with the scam.

Intentional confusion: Scammers may purposefully complicate their trails to confuse investigators. Some tactics that they use include creating fake logs or trails, duplicating accounts or adding more accounts into the execution of the scheme, and performing activities that may lead away from the actual scam.

The loop

Certain scams are recurring in nature. Akin to playing "Whack-a-mole", one disappears and pops up again, using the same modus operandi but with different fronts and tactics, towards different targets.

This is informed by the UNDP's Scam Journey Map. It highlights an important part of the scam journey not covered in other frameworks, a "re-scamming" element, whereby the scammer reengages in other scam activities after successfully extracting funds. The scam process is therefore not always one-off nor completely linear. Depending on the circumstances, the Loop may return to various stages, such as Operational Setup, Establishment of Contact and the Luring, Baiting and the Ask.

The Loop is not considered a separate stage of the Scam Anatomy, and functions as an element to highlight parts of the process that may be repetitive.

Cashing out

In this stage, perpetrators retrieve their illegally obtained funds successfully without being traced, and reintroduce the money legally into financial systems via money laundering. The

[18] Izuakor (2019)

[19] TOR is a web browser enabling enhanced browsing privacy and anonymity. Users can access blocked content, bypass censorship, and clear history, cookies automatically after each session, defending against browser fingerprinting.

objective of this process is to break the link between the "dirty" money and its illicit origins and convert it into "clean" money, enabling scammers to use the funds without attracting the attention of law enforcement.

Money laundering, regardless of the type and form of asset (e.g. fiat money, stocks, cryptocurrency or properties) is usually done through three interconnected stages:

Placement: In this stage, the perpetrators attempt to move the illegally obtained funds away from the original source and introduce it into a legitimate financial system that is regulated by authorities like the Bank Negara Malaysia (BNM), the central bank. This is also when criminals are typically more vulnerable to discovery by law enforcement as they attempt to move bulk amounts of money which could trigger Anti-Money Laundering (AML) protocols[20].

Layering: This stage of the money laundering process is more sophisticated, as it often involves multiple techniques and transactions to hide the origins of the money. The goal is to complicate tracking efforts by authorities through obscuring the trails leading to the criminal. This is typically where money moves across complex cross-border networks using offshore accounts, shell corporations, currency conversions, and even blending illegitimate funds with legitimate business activities[21].

Integration: In the last step of the money laundering process, scammers successfully integrate the money back into the economy, appearing as legitimate funds. This enables them to return the funds to their possession to make them available for utilisation for both regular and criminal activities[22].

2.3. Applications of the scam anatomy

Across the modus operandi of various scam types, we find that the structures of most scam operations are designed in a manner that aligns with the seven-stage Scam Anatomy framework. Appendix 2 illustrates a typical scam operation by breaking down the case of online romance scam into different stages using the Scam Anatomy that we developed.

Online dating platforms and social messaging apps have changed the way people find potential romantic partners, making it more convenient and accessible. With increased popularity of online dating, scammers have found it lucrative to exploit genuine search for connections for financial gain. In online romance scams, romantic connections are fabricated to emotionally manipulate the victims, with the goal of swindling them. In January 2026 alone, 100 love scam cases were recorded by the PDRM, with total losses amounting to RM3.5 million[23].

As shown in Appendix 2, the progression of online romance scam at each stage is not linear from start till end. There is a tendency to loop back into earlier stages depending on how the

[20] Lexis Nexis (n.d.)
[21] LSEG Risk Intelligence (n.d.)
[22] BNM (n.d.)
[23] MalayMail (2026)

relationship and extraction develop. This aligns with the Scam Anatomy, as indicated above, that it allows for looping back to different stages, since not all scams follow a linear process.

The Scam Anatomy can also be applied to other types of scams such as product and services scam[24], online job scam, pump and dump scam and more. While some exhibit slight variations in the process, the core elements remain the same. For instance, in a pump and dump scam case, in the "Ask" phase, instead of directly requesting money from the victim, the scammers urge the victims to buy and hold the shares or crypto coins. This drives the price upwards until it peaks, at which point the scammers dump their remaining shares to sell, and cash out.

[24] According to Keepnet, a cybersecurity solutions company, a product and services scam occurs when perpetrators "*pretend(s) to be a real seller or service provider to trick (victims) into paying for something fake.*"

3. Issues, actors and initiatives across the scam lifecycle in Malaysia

Scam cases in Malaysia have shown a clear upward trajectory from 2023 to 2025. As seen in Table 2, the number of scam cases nearly doubled between 2024 and 2025, a sharp increase that is worrying. What is being done about it, and what is lacking in our response? In this section, we use the Scam Anatomy framework to examine core issues along the scam lifecycle and look at regulatory and non-regulatory measures currently in place in Malaysia. Through an examination of the existing measures, we identify critical gaps to be addressed.

Table 2: Statistics of the number of online scam cases from 2023 to 2025

Year	Number of Online Scam Cases
2023	34,497
2024	35,368
2025 (as of November)	67,735

Source: PDRM

As discussed in the previous section, a scam operation does not begin when it is first detected, and end when the scammers exit the scene. Significant activities occur throughout the entire chain, spanning from the pre-scam to the post-scam stages.

Based on the Anatomy, we identify specific issues associated with each stage and the relevant stakeholders[25]. The main issues refer to the key vulnerabilities and areas of concern associated with each stage of the scam operation. From there, we provide a (non-exhaustive) list of important governmental and non-governmental actors that play a role in enabling, regulating, preventing, or responding to activities within the respective stage.

Table 3: Expanded Scam Anatomy including issues and stakeholders in Malaysia

Stage	Main Issue(s)	Key Actors	Lead/ Supporting Governmental Organisations
Foundation Work	Data privacy and security	- NACSA - JPDP - MCMC - CSM	NACSA, MCMC, CyberSecurity Malaysia

[25] The "Loop" is omitted from the visualisation for simplicity; however, it should be noted that it exists.

Operational Setup	Authentication and verification by service providers	- Application Service Providers (ASPs)[26] - Content Application Service Providers (CASPs)[27] - AI service providers - Telecommunication companies - MCMC	
Establishment of Contact	Authentication and verification by individuals Fraud detection and algorithmic amplification by service providers	- Victims - ASPs - MCMC	
Luring, Baiting and the Ask	Individual awareness on verification and response	- Victims - Civil society organisations - Government (MoE, MoHE, etc.) - Financial Institutions (BNM, SC, etc.)	
'Hurrah' Moment	Consumer protection	- Financial institutions - Consumer protection organisations (FOMCA, MCCA, etc.) - Victims	
Disappearing Act	Law enforcement	- PDRM - NACSA - ASPs	
Cashing Out	Money laundering	- BNM - PDRM - NFCC - SC - MACC - Financial institutions	

Source: Authors' visualisation

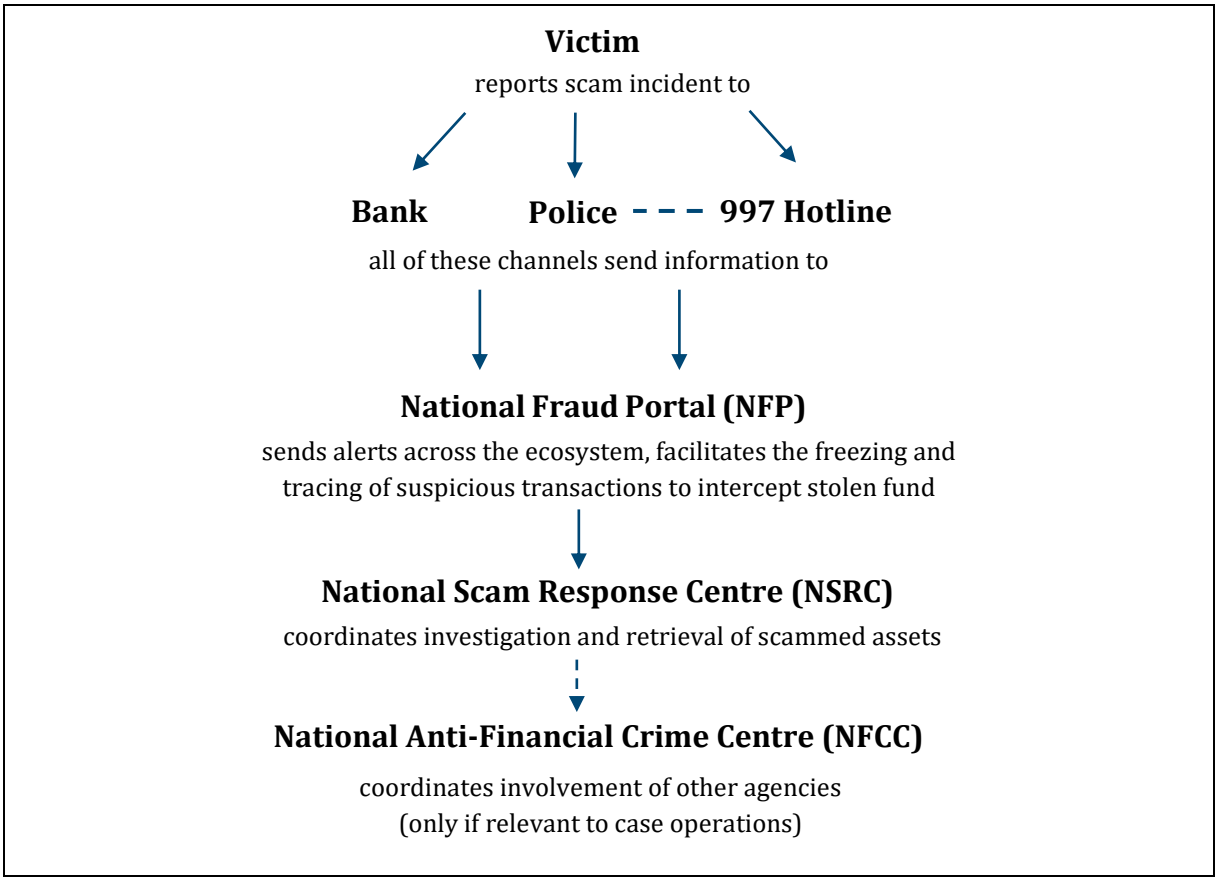
[26] ASPs "provide particular functions such as voice services, data services, Internet access and messaging services. Applications services are essentially the functions or capabilities which are delivered to end-users. These are retail services." (MCMC (2023), p4)

[27] CSPs "represent a special subset of applications service providers such as television and radio broadcast services, and services such as online publishing (currently exempt from licensing requirements) and the provisioning of information services." (MCMC (2023),p4)

Much coordination needs to happen among the different actors. The scam reporting flow gives an idea of how agencies coordinate to respond to a scam incident. As shown in **Error! Reference source not found.**, when a victim encounters a scam and a transfer of funds has occurred, they must immediately notify either the PDRM (via the 997 hotline) or the relevant bank. Upon receiving the report, the authorities will transmit the information to the National Fraud Portal (NFP)[28], which then issues alerts across the financial ecosystem to halt the flow of funds and freeze assets in the shortest time possible.

Subsequently, the National Scam Response Centre (NSRC), led by the PDRM, coordinates the investigation and the process of recovering the scammed assets. If a joint operation is required, the National Anti-Financial Crime Centre (NFCC) becomes involved to coordinate the participation of other law enforcement agencies including the Malaysian Anti-Corruption Commission (MACC), BNM, the Companies Commission of Malaysia (SSM), and the Securities Commission (SC).

Figure 2: Scam reporting process in Malaysia



Source: Authors' visualisation

[28] See Appendix 9 for more information about the NFP

Some of this coordination has borne fruit. According to BNM, since the establishment of NFP in 2024 to coordinate among financial institutions, it has managed to reduce the time taken to trace stolen funds by 75%[29]. As scam numbers go up, the sophistication of scam response has to increase as well.

In the next subsections, we will take a deeper look into different stages of the scam lifecycle to understand the measures in place as well as existing gaps, to set the context for recommendations to follow.

3.1. Foundation Work

Core issue: Data privacy and security

Key actors: National Cyber Security Agency (NACSA), The Personal Data Protection Department (JPDP), Malaysian Communications and Multimedia Commission (MCMC) and CyberSecurity Malaysia (CSM)

Foundation work sets the stage for a scam to happen. As shown in the previous section, scammers rely on information to design and craft specific scam activities. A large part of this involves the profiling of potential targets, through obtaining large troves of personal and behavioural data.

Data privacy and security is therefore the core issue of this stage. Data privacy refers to the safeguarding of an individual's personal and sensitive information from unauthorised parties[30], while data security "encompasses a set of related standards, technologies, frameworks, and processes that focus on protecting data from unauthorized access and corruption throughout its lifecycle"[31]. Data must be protected starting from the moment it is collected, to when it is stored, shared or transmitted – with strict compliance to security control measures, proper security architecture in place, and proactive security monitoring[32]. Any negligence throughout the data lifecycle of data allows the possibility of data breaches.

Verizon's 2020 Data Breach Investigations Report revealed that 86% of data breach cases are found to be motivated financially[33], and made a link between data leaks and illicit activities such as financial scams, fraud and extortion.

In Malaysia's context, the problem of data breaches is significant and growing in severity. Gogolook's Whoscall 2024 Report highlights a concerning finding: Malaysia ranked first in Asia in terms of data leakage rates — 72.5% of Malaysian Whoscall users who performed status checks

[29] BNM (2025b)
[30] Alafaa (2022)
[31] Wang (2025)
[32] Ibid.
[33] Bassett et al. (2020)

through the ID Security feature found that their personal information had been compromised[34]. In addition, according to the latest Cyber Incident Quarterly Summary Report by MyCERT for the third quarter of 2025[35], there is an increase of 38% in the data breach incidents received by the Cyber999 Incident Response Centre in Q3 2025, as compared to Q2 2025.

Besides leakages through data breaches and malicious activity, a separate issue is digital hygiene at an individual level. BNM in the Financial Capability and Inclusion Demand Side Survey 2024 suggested that while the 2024 figures indicate positive progress in terms of Malaysians' digital hygiene level, further improvements are still needed[36]. The examples cited, inter alia, that only 39% of Malaysians surveyed[37] were mindful about website security before making transactions, while the global average stands at 66%. Besides, more than one in 10 Malaysians reported sharing confidential data such as bank account passwords with their close friends. Such practices expose individuals to data privacy and security risks, and following that, financial scams.

Regulatory measures and non-regulatory measures in place

In dealing with issue of data privacy and security, we can examine the ecosystem of regulatory measures governing data in its two main categories: security and privacy. For the former, in ensuring that data remains safe and intact, the Computer Crimes Act 1997 (CCA), the Cyber Security Act 2024 (CSA), the Communications and Multimedia Act 1998 (Amendment 2025) (CMA), and the upcoming Cyber Crime Bill (at the time of writing, the bill had been passed in the lower house of the parliament) are the key legislations that can be invoked. For the latter, the Personal Data Protection Act 2010 (Amendment 2024) (PDPA) safeguards consumers' personal data in the commercial transactions space. Nevertheless, it is important to note that the Act is limited to the private sector and does not extend to the public sector.

On the non-regulatory front, members of the public, businesses and organisations, as well as government agencies in Malaysia, can turn to CyberSecurity Malaysia (CSM), the national cybersecurity specialist agency, for support in safeguarding their systems. CSM was established specifically to develop a more resilient and secure cyber ecosystem in Malaysia[38].

For details on the regulatory and non-regulatory measures, refer to Appendix 3 and Appendix 4.

Gaps

Upon examination, we find that the regulatory measures appear to be sufficient and comprehensive in addressing the core issue highlighted earlier in this section. While we acknowledge that certain legislation, particularly the CCA (1997), has become outdated, a new

[34] Whoscall MY (2025)
[35] MyCERT (2026)
[36] BNM (2024)
[37] With a sample size of 3,587 respondents
[38] For a detailed list of the services provided, visit https://www.cybersecurity.my/

Cybercrime Bill was passed in parliament in July 2026 to replace the CCA, to cater to new developments in the area of criminal activity in the cyberspace.

Cybersecurity capacity gaps in Malaysian businesses: Basic digital protection remains an issue for many businesses, leaving them vulnerable to cyberattacks. According to the International Association for Counterterrorism and Security Professionals Centre, a significant number of businesses are still operating on outdated software versions with known vulnerabilities, which become entry points for cybercriminals to exploit[39].

Such a situation could be attributed to several possible causes. First, many businesses do not allocate a dedicated budget to hire a team of cybersecurity experts to safeguard their operations from cyberattacks[40]. Second, even when sufficient budget is available, Malaysia is currently facing a critical shortage of cybersecurity professionals. According to NACSA, the country faces a shortage of roughly 10,000 skilled workers in the cybersecurity domain[41]. Echoing this view, Fortinet Southeast Asia noted that 84% of organisations in Malaysia reported difficulties in securing qualified cybersecurity experts[42]. This shortfall significantly increases the vulnerability of organisations to data breaches.

Enforcement issues: While comprehensive laws and policies are in place, enforcement remains a significant challenge. As highlighted in a press statement by the Malaysian Bar, the "perceived absence of visible or timely enforcement action in response to previous high-profile data breaches undermines public trust,"[43] pointing to enforcement shortcomings among the relevant authorities. In the absence of strong enforcement measures, incidents of data breaches, including the open sale of personal data on the dark web, are likely to continue unabated.

3.2. Operational Setup

Core issue: Authentication and verification by service providers

Key actors: Application Service Providers (ASPs), Content Application Service Providers (CASPs), AI service providers, telecommunication companies, MCMC

The Operational Setup phase is about getting "ammunition" ready to launch a scam attack. The preparation includes (but is not limited to) the creation of fake user profiles, content and platforms to create façades as a front for deception. Core issues here are the difficulties in authentication and verification of digital identity and the origins of content, particularly at a service provider level.

[39] Subra (2025)
[40] Ibid.
[41] BERNAMA TV (2025)
[42] Nik Faiz Nik Ruzman (2025)
[43] Malaysian Bar (2025)

From a cybersecurity perspective, authentication refers to "verifying the identity of a user, process, or device"[44]. Authentication and verification can be applied at different levels, as elaborated below.

Authentication and verification of prepaid SIM card owners: As mentioned in Section 2.2, an active mobile number is often needed as a basis for verification when creating user accounts across many services. The ease of obtaining SIM cards in Malaysia is therefore an issue. At the time of writing, pre-registered prepaid SIM cards can be easily purchased on e-commerce platforms, with no limits on the quantity bought. This is a concern recognised by MCMC[45]. Pre-registered SIM cards are linked to the registrant's name, hiding the real identity of scammers behind the SIM card.

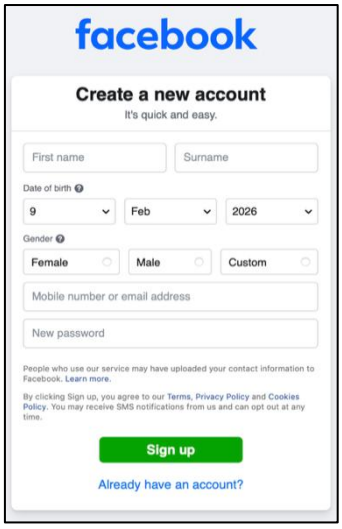
Besides purchasing pre-registered SIM cards, perpetrators can use stolen or leaked personal data to register SIM cards without the victim's knowledge. SIM card swap, also known as SIM card replacement, is another way to operate a SIM card under another person's identity. This happens when the scammer obtains one's personal details and requests to replace a SIM card with his or her network provider, under the pretext of a missing phone. Once the scammer receives the replaced SIM card, full control of the mobile number would then fall under the scammer[46].

When a SIM card is implicated in a scam, the registered individual whose name appears in the database would become the first suspect to be investigated, despite being not involved in the scam. This is known as secondary victimisation, where innocent people are being investigated, blacklisted or labelled as accomplices[47].

Authentication and verification of user profiles: Due to the high penetration rate of social media platforms (with 85 percent of Malaysia's population already connected, as of October 2025[48]), social media is a natural site for scammers to establish contact with potential victims. Most social networking platforms request minimal information when one tries to sign up for an account (see example in Figure 3). The ease of profile creation reduces friction for scammers to reach a high number of people; the usage of scripts or bots can also automate this process.

[44] National Institute of Standards and Technology (n.d.)
[45] MCMC (2026a), page 115
[46] Maybank (n.d.)
[47] Abdul Hamid (2025)
[48] We Are Social (2026)

Figure 3: Snapshot of the Facebook registration page that comes with the tagline "it's quick and easy"



Authentication and verification of AI-generated content: The difference between AI-generated content and human-made content is getting harder to discern. AI authentication, which refers to "determining when content is AI-generated or otherwise verifying the validity or provenance of layers of the AI value chain"[49], is therefore increasingly important. Labelling of AI content is one such technique.

Regulatory measures and non-regulatory measures in place

Regulatory and non-regulatory measures address the issues outlined above at two levels – for SIM cards, and for ASPs[50] and CASPs[51].

First, with regard to SIM cards, we find that the verification process for registering a new prepaid SIM card has been strengthened. Since 26 February 2026[52], new prepaid SIM card users have been required to undergo an additional layer of verification through biometric authentication and MyDigital ID.

In addition to this regulatory measure, several non-regulatory initiatives have also been introduced to allow for more efficient verification. For example, under the MyIDVerify initiative, prepaid SIM card users are now able to review and confirm all prepaid numbers registered under their National Registration Identity Card (NRIC), a process known as "whitelisting". Should there be any numbers that have been fraudulently or erroneously registered under their identities,

[49] Information Technology Industry Council (2024)
[50] E.g. social media platform and internet messaging services
[51] E.g. internet web casting and streaming platforms
[52] Commission Determination on the Mandatory Standards for the Registration of End-Users of Prepaid Public Cellular Services, Determination No.1 of 2026.

users may report them to the relevant telecommunications provider, thereby preventing the potential misuse of their identities by scammers.

For telecommunications providers, a federated number verification system known as Number Verification API has also been introduced to enable local banks and online retailers to verify and authenticate the identity of mobile users[53]. This system is the result of a collaboration among five major telecommunications companies in Malaysia, namely CelcomDigi, Maxis, U Mobile, Telekom Malaysia, and YTL Communications.

Second, for ASPs and CASPs, many issues arise within their domain during this stage, particularly fraudulent user profiles and content. As a regulatory measure, MCMC has mandated social media licensing since 1 January 2025 for ASPs with eight million or more registered users in Malaysia. As a result, these ASPs are now lawfully subject to statutory provisions, licence conditions, and regulatory directions issued by the MCMC.

In the same vein, from a content regulation perspective, the Online Safety Act 2025 (ONSA) came into force in 2026 to regulate harmful content by imposing duties and obligations on CASPs and ASPs. Importantly, "content on financial fraud" is listed as one of the Act's priority harmful content categories and is therefore subject to additional and prioritised controls. Coupled with the social media licensing framework, ASPs can now be held accountable under the ONSA for their obligations relating to harmful content on their platforms.

Six months after the enforcement of the ONSA, the MCMC introduced additional requirements for licensed ASPs and CASPs through the Risk Mitigation Code issued under the Act. Pursuant to the Code, licensed service providers are required to implement appropriate labelling or watermarking measures to indicate "generated or manipulated images, audio or video that closely resemble real persons, objects, places, entities or events" on their platforms.

The Risk Mitigation Code also mandates advertiser verification measures. Under the Code, licensed service providers are required to verify advertisers offering goods or services against Government-issued records before permitting them to publish advertisements on their platforms.

Appendix 5 provides further details on relevant regulatory measures.

Beyond the regulatory measures by the state, some platforms have also implemented their own measures to address these issues. To illustrate, most major social media platforms are now equipped with anti-scam tools, though these vary in form and implementation. For instance, Meta has recently introduced new features across Facebook, WhatsApp and Instagram to combat sophisticated scams on its platforms. Most of these features integrate the use of AI to analyse and alert consumers about suspicious interactions[54].

[53] Fam (2025)
[54] Meta Newsroom (2026)

Starting April 2026, Google is implementing new certification requirements for financial services advertisers targeting Malaysia. Selected financial products and services advertisers must complete a verification process, proving authorisation from Malaysian authorities like SC, BNM and Labuan Financial Services Authority before they are allowed to run ads on Google's platforms[55].

Upcoming initiatives

The government has proposed several legal reforms that are expected to be completed by the end of 2026. Recognising the risks posed by AI, the Ministry of Digital is currently developing an AI Governance Bill as part of Malaysia's broader AI legislative framework. Once enacted, the bill will place the developers and deployers of AI under greater regulatory oversight[56]. This would minimise AI-related risks while promoting the responsible use of AI.

While the proposed AI Governance Bill primarily targets AI service providers, the recently passed Cybercrime Bill seeks to hold individual offenders accountable. Among its proposed provisions is the prohibition of generating realistic synthetic or manipulated content intended to facilitate crime.

Gaps

We commend the government's efforts in introducing the above regulatory measures, particularly the focus placed on ASPs, CASPs and telecommunication service providers. While it is still too early to conclusively assess their effectiveness due to the short implementation period, these measures mark an important step towards tighter regulation of platforms that have high user bases and therefore a higher scale of potential harm. Nevertheless, gaps still remain in the following:

Lack of regulation on the sales of pre-registered prepaid SIM card and e-SIM: Although the onus of ensuring proper prepaid SIM card (including e-SIM) registration falls on the telecommunications companies, the open sale of pre-registered prepaid SIM cards should be cracked down. This calls for more stringent regulations and enforcement on the distribution channels of pre-registered prepaid SIM cards, including agents and street-level dealers[57], as well as on e-commerce platforms. For example, a run-through of the lists of prohibited items available on major e-commerce platforms in Malaysia reveals that there are no specific prohibitions on the sale of pre-registered prepaid SIM cards.

[55] The Star (2026)
[56] Ong, Chia, and Lim (n.d.)
[57] Alias (2026)

3.3. Establishment of Contact

Core issues: Authentication and verification by individuals; fraud detection and algorithmic amplification by service providers

Key actors: Victims, ASPs, MCMC

The Establishment of Contact stage is set in motion when the scammers attempt to establish a contact point with the targeted victim, through fake user accounts, content or platforms set up in the previous stage. The critical issues here are therefore the need for ASPs to proactively detect scam activity and reduce algorithmic amplification of problematic content.

Fraud detection and algorithmic amplification[58]: ASPs play an outsized role at this stage, where the point of contact happens. As they have comprehensive data about interactions happening on their platforms and the ability to conduct effective predictive analysis, they are well-placed to set up fraud detection mechanisms for suspicious interactions. This involves the blacklisting of fraudulent profiles and removing scam-related advertisements or content.

Findings of a research report by Barracuda, a cybersecurity company, alongside researchers from the University of Chicago and Columbia University, reveal that perpetrators now exploit AI to test advertising phrases that are more likely to 1) bypass detection mechanisms and 2) be clicked by targeted victims on platforms. This practice resembles the A/B testing which is usually performed in traditional marketing[59]. Compounding the problem, the ad-personalisation systems on social media platforms tailor content to user preferences, delivering more scam-related ads to users who have clicked on scam ads. This will increase the likelihood of targeted users falling for scams.

Scam activities are prevalent across different social media platform. Meta is not the only social media giant attracts scam activity, even though it accounts for more than half (56%) of the detected scams across social media platforms. An article of Global Anti-Scam Alliance published in 2025 reveals that YouTube (26%), X (7%) and Reddit (5%) are likewise among social media platforms that are popular among scammers[60].

Regulatory measures and non-regulatory measures in place

At this stage, fraudulent content is already circulating within the online space, and the focus shifts towards preventing it from reaching potential victims. To achieve this, two key mechanisms under the CMA 1998, namely content takedown requests and website blocking, are often relied upon.

[58] The promotion of content to users by algorithms based on their behaviour
[59] Hao (2025)
[60] Corrons (2025)

For the former, the CMA designates the MCMC as the primary authority responsible for submitting content removal requests to online platforms. These requests are mainly made following MCMC's proactive monitoring and complaints received from the public. According to the Ministry of Communications, from 1 January until 19 April 2026, the MCMC received a total of 203,918 takedown requests from the public, in which approximately 30% of the requests were related to scam content[61].

With regard to website blocking, the CMA gives authority and power to MCMC to block websites by instructing internet service providers (ISPs) such as Unifi and CelcomDigi to restrict users' access. This has been applied in the context of blocking scam-related websites. MCMC disclosed in 2024 that in a period of about 2.5 years, it had blocked 316 scam and illegal investment websites[62].

Beyond these regulatory measures, platforms themselves have also implemented various content moderation mechanisms and technical tools. For instance, built-in spam filters on email platforms prevent spam, phishing, and malware from reaching users' inboxes, while messaging applications often include features that warn users about unknown contacts. Notably, major email platforms such as Gmail[63] and Outlook[64] employ machine learning to detect and flag spam by identifying patterns within their large and continuously expanding datasets.

Content moderation can also happen at the network level, conducted by the telecommunication companies. An example is U Mobile, which stated that it successfully blocked over 265 million scam calls and fraudulent SMS messages across its 5G and 4G networks in Malaysia before they reached end users[65].

For social media, most of the major social media platforms such as Meta, TikTok and YouTube come with community guidelines that prohibit harmful content (including fake accounts), with fraud- and scam-related content being a significant part of the guidelines. In general, these platforms claim to reject any form of deceptive practices by adopting technology to proactively detect the content and, if necessary, having trained reviewers to manually review the potential violations.

In cases where fraudulent content reaches users despite these content moderation efforts, user-facing scam detection tools provide an additional layer of protection. In March 2026, Meta launched new anti-scam tools for users on their platforms such as Facebook, Messenger and WhatsApp. These tools use integrated AI technologies to aid users in identifying potential scams and provide guidance on safety measures that users can take[66].

---

[61] BERNAMA (2026)
[62] MCMC (2024)
[63] Kumaran (2022)
[64] Kontorskyy (2024)
[65] U Mobile (2025)
[66] Meta Newsroom (2026)

Gaps

From the above, we can see that the **regulatory measures are largely reactive in nature**. Only upon the discovery of harmful content do subsequent steps, such as content takedown requests and website blocking, follow. This allows harmful content that escapes early detection to remain undiscovered and continue proliferating in the online space, potentially reaching and affecting more individuals before any intervention takes place, especially given that scam syndicates operate around the clock.

Platforms are not disincentivised to curb scam advertising: Despite having community guidelines that prohibit harmful content, scam ads still run rampant on social media platforms. One of the largest factors of such proliferation is the business model of the platforms which rely on income from advertising[67].

For example, Reuters exposed that internal documents from Meta projected that one tenth of its total annual revenue in 2024, equivalent to $16 billion, were from publishing ads for scams and banned goods. The same report highlighted that for three years, the company failed to identify and prevent advertising related to scams from reaching billions of users across Meta's main social media applications such as Facebook, WhatsApp and Instagram. On a daily basis, users using Meta's platforms were exposed to approximately 15 billion "higher risk"[68] scam ads. It is worth noting that the cost of any regulatory settlement involving scam ads is often far lower than the revenue earned by platforms from hosting such ads[69].

While internal warning systems are found in place for most platforms, the threshold for takedowns is often too high. To continue with Meta as an example, the fraud detection system only triggers when the system determines that it is at least 95% certain that the advertisement is problematic. Below the 95% threshold, even if Meta is fairly convinced that the advertiser is a likely scammer, it still allows the advertisement to be shown, albeit with a higher advertising fee. While this is framed as a discouragement to place scam ads, effectively Meta is earning a higher rate from harmful advertisements[70] .

At the time of writing, as mentioned above, Meta has made new pledges in their fight against scams. Nevertheless, as the business model of the platforms remain unchanged, the profit motive is still there. Relying solely on the goodwill of these platforms may result in arbitrary and inconsistent implementation of the anti-scam measures.

[67] From roundtable discussion
[68] Defined as ads showing clear signs of being fraudulent
[69] Horwitz (2025), Roundtable Discussion
[70] Ibid.

3.4. Luring, Baiting and the Ask

Core issue: Individual awareness on verification and response

Key actors: Victims, Civil Society Organisations (CSOs), Government (Ministry of Education (MoE), Ministry of Higher Education (MoHE), etc.), Financial Institutions (BNM, SC, etc.)

During this phase, scammers typically manipulate human psychology by employing social engineering tactics, exploiting cognitive biases and preying on emotions to provoke a response from the victims. According to the Elaboration Likelihood Model introduced by Petty and Cacioppo in 1986[71], scammers present messages in ways that force victims to make snap decisions that rely on emotions rather than logic to influence their decisions[72]. While victims' awareness is the main issue perpetuating the problems at this stage, there are several facets to the problem – the ability to authenticate and verify information, the proliferation of unreliable information, as well as response capabilities and psychological biases.

Proliferation of unreliable third-party information: Malaysians are exposed to a lot of financial misinformation and disinformation online. In 2024, the SC received 4,859 complaints regarding misleading financial claims[73]. Many of these cases were linked to content on platforms like TikTok and Telegram, where some scammers pose as financial content creators, or also known as "finfluencers", luring victims by flaunting their wealth and flashy lifestyles, or offering promises of getting rich quick.

Deepfakes are also weaponised to lend credibility and legitimacy towards false claims. Recent cases in Malaysia include deepfakes of members of the royal family such as the Yang di-Pertuan Agong, prominent politicians like the prime minister[74], and public figures including actors and business tycoons[75]. The sophistication of the content increases the risk to investors because Malaysian investors rely heavily on third-party sources that they perceive to be credible when making financial decisions, as observed by the SC[76].

Most users do not verify information they consume online: Malaysians generally indicate high confidence in their ability to identify scams. In the National Scam Awareness Survey 2024 report published by CelcomDigi, covering a sample size of 10,893 respondents, 87% of respondents self-reported high awareness of scams[77]. However, that confidence about identifying scams does not necessarily indicate the ability nor the inclination to verify and authenticate false

[71] Petty and Cacioppo (1986)
[72] Shang et al. (2023)
[73] SC (2025)
[74] The Star (2025)
[75] BERNAMA (2025)
[76] Yew Yee Tee (2025)
[77] CelcomDigi (2024)

information. In Department of Statistics Malaysia (DOSM)'s ICT Use and Access by Individuals and Households Survey Report 2024, less than 30% of Malaysians surveyed verify the reliability of information found online [78]. While it may be generally caused by inadequate digital literacy and lack of access to fact checking tools, cybersecurity experts also highlight that reliance on social media as a dominant source of information exacerbates the spread of hoaxes and scam content[79].

Scam targets' lack of ability to respond to manipulation and coercion: Depending on the type of scam, the luring and baiting phase of a scam operation may either take weeks or just minutes. Regardless of the duration, it is up to the targets to resist the tactics of the scammer, especially under manufactured urgency. Most targets are ill-equipped to deal with scammer manipulation and coercive tactics. According to a study done by RinggitPlus in 2024, 32% of the 3,385 surveyed respondents do not know how to react to fraudulent behaviour such as impersonation and false notifications[80]. A separate study by Ipsos Malaysia also found that less than half of 1,000 Malaysian scam victims they surveyed sought help from the authorities[81].

This highlights a nuanced situation: knowing about scams alone is not enough in the fight against modern, sophisticated scams. Being able to convert that information on cyber financial scams towards action by knowing how to respond to scams tactics, and how to seek for help is equally important.

Regulatory measures and non-regulatory measures in place

As most of the issues in this phase are psychological in nature, there is a limited number of laws and policies that address them. The Guidance Note on Finfluencers from the SC[82] is one attempt to regulate misleading financial content. Unless they are licensed by the commission, finfluencers are no longer allowed to promote any capital market product, including cryptocurrencies and trading platforms on social media.

The issue of public awareness centres on whether members of the public are adequately informed about scam-related risks and preventive measures. Upon examination, we find that the public is generally well served in this regard, given the numerous awareness campaigns conducted by various stakeholders. The nature of these campaigns varies; some are one-off initiatives, while others are long-term in nature. A detailed list of ongoing awareness campaigns is available in Table 8 in Appendix 6.

Beyond these awareness campaigns, entities like SC have been actively disseminating information to the public. This includes information on new forms and modus operandi of scams via media releases, industry blasts to intermediaries, and other communication channels. Some of the scam alerts issued previously include the incident of the SC public register being cloned

[78] Department of Statistics Malaysia (2025)
[79] Yuen Meikeng (2025)
[80] RinggitPlus (2024)
[81] Nurqalby Mohd Reda (2023)
[82] Securities Commission (2024a)

and other types of scams such as those involving deepfakes and impersonation, fake guarantee deposits and pre-IPO investments[83].

On top of awareness, the general public also has access to a variety of tools provided by different stakeholders and authorities to authenticate and verify information. The type of information ranges from suspected mule accounts, unregulated financial entities or schemes, as well as unlicensed financial institution and money lending companies (see Table 9 in Appendix 6 for more details).

There have also been digital literacy and financial literacy interventions within the formal education system to equip students with the knowledge and skills. While the initiatives listed are not exhaustive, it spans across primary and secondary school systems, targeting both students and teachers (see Table 10 in Appendix 6).

Gaps

Difficulty in determining the effectiveness and adaptability of literacy modules, fact-checking tools and awareness campaigns: For primary and secondary schools under the purview of the MoE, the implementation of many initiatives such as the National Cyber Ethics Module and the *Program Kejurulatihan Pengurusan Kewangan Peribadi Guru* (Train-the-Trainer Programme: Personal Financial Management for Teachers) has only just been introduced. It is difficult to determine the effectiveness of these programs, as outcomes of pilot sessions have not been made public. These issues are not just limited to newly established modules – it is also difficult to determine the effectiveness of programmes run, as impact reports are not usually published publicly.

Furthermore, the threats of cyber financial scams are evolving as cybercrime becomes "increasingly industrialised". People are become more vulnerable to new threats, but the digital education policies and syllabi are not adapting fast enough to keep up with scammers' tactics and schemes[84]. Supporting this, the Home Minister stated that changing tactics of syndicates and low levels of digital literacy are among the main factors that scam cases are on the rise despite running 10,400 prevention activities nationwide in 2024[85].

Fragmentation and gaps in outreach: Awareness campaigns are fragmented, and there is limited multilingual outreach [86]. Stakeholders also noted that both KD and Ministry of Communication have digital literacy modules, but they are not well facilitated nor streamlined to provide a mutually-aligned and comprehensive impact towards the understanding of the public[87].

[83] Securities Commission (2024b)
[84] Stakeholder interviews
[85] The Straits Times (2025)
[86] Atan et al. (2025)
[87] Stakeholder interviews

Inadequate fact-checking by platform service providers, outsourcing the work to users: According to DOSM, only 29.5% of the surveyed users who participate in social networks use the Internet to verify the reliability of information found online[88]. This shows that majority of users do not go out of their way to verify information outside of social networking platforms. This presents plenty of opportunities for scammers to misinform and disinform potential victims on social networking sites because the information users receive on social media is not being actively fact-checked.

This scenario highlights a stark gap between existing fact-checking initiatives and user habits. Currently, most social media users in Malaysia have to rely on external tools, such as Sebenarnya.my provided by the Malaysian government, to fact-check information they receive from sources such as social media platforms.

There is a need for independent, professional fact-checkers to actively verify content on these social media platforms. Previously, Meta had a third-party fact-checking programme, where they partnered with independent organisations to run fact-checks on platform's content. However, they stopped the programme in favour of the Community Notes model (pioneered by X), citing freedom of speech. The Community Notes model allows social media users to add context to content that they believe may be misleading or inaccurate, to warn other users of misleading content[89]. However, experts have raised concerns about this feature.

Based on the implementation of Community Notes on X, the Institute for Strategic Dialogue identified several issues when analysing the effectiveness of the user-driven feature. For example, community notes cannot keep pace during high-volume crises such as natural disasters. Logs recorded a median lag of over 15 hours between the posting of misleading content and the addition of a helpful Community Note. In crises, the gap widens to an average delay of about 46 hours. While the Community Notes feature helps reduce user engagement with potentially misleading content, its effectiveness is hindered as most views and engagement on a post occurs within the first few hours of publication[90].

This suggests that such a feature should serve only as an additional layer of protection, rather than replacing existing fact-checking programmes altogether. In this regard, TikTok provides a stronger example by introducing its Footnotes feature while retaining its third-party fact-checking programme alongside other fact-checking measures.

[88] Department of Statistics Malaysia (2025)

[89] To date, roll-out for Meta has begun in the US, with planned expansion to countries outside of the US in the future.

[90] Institute for Strategic Dialogue (2025)

3.5. Hurrah Moment

Core issue: Consumer protection

Key actors: BNM, Financial institutions, consumer protection organisations (Federation of Malaysian Consumers Associations (FOMCA), Malaysia Cyber Consumer Association (MCCA), etc.), victims

One of the most critical points in the scam process is the instance of money transfer between the victim and scammer. It is also the last point of contact between the scammer and the victim. Consumer protection is the key issue here, from the perspectives of 1) financial institutions responsible for safekeeping funds and processing transactions, and 2) consumer protection organisations that provide frontline response when victims reach out for support. Problems that exacerbate the situation include the following:

Frictionless real-time transactions increase vulnerabilities: In Malaysia, the DuitNow system uses QR codes and enables instant transfers to registered accounts. Real-time payment systems are designed to enable near-instantaneous money transfers between banks and financial institutions. These systems allow funds to be sent and received within seconds, at all hours of the day. This is much faster compared to the past, when legacy banking systems had multi-day processing times.

While frictionless payment systems provide greater convenience and a better user experience, they can also be exploited by scammers. The World Bank highlights that the same features of fast payment systems benefit users and scammers alike. One of the main issues is posting speed, making it difficult for payment service providers and financial institutions to run checks on the transactions, considerably shortening the available time to respond. This is because the scammer will have access to the funds immediately and can move the funds rapidly between accounts[91]. The removal of transactional barriers also leaves users with less time to reflect on their actions, thereby reducing the opportunity to reconsider potentially risky transactions[92]. Payment finality features of fast payment systems also pose a problem, as money transfers cannot be easily reversed.

Scammer's coaching: While digital finance systems do come with security measures, the victims themselves are evading technological safeguards through coaching from scammers. Through this, efforts by financial institutions are rendered ineffective. Two different types of coaching have been reported by Malaysian bank officials[93]: 1) coaching from scammers to bypass questions from bank officers to confirm suspicious transactions, and 2) coaching to structure transactions in a

[91] World Bank Group (2023)
[92] Kunkel (2025)
[93] Jassmine Shadiqe (2025)

way that dodge red flags in the banking system, breaking large amounts into smaller, seemingly routine transfers made over time to multiple mule accounts.

Regulatory measures and non-regulatory measures in place

Generally speaking, in cases of fraudulent activities, prosecutors will invoke Sections 415, 420, and 424 of the Penal Code to charge and prosecute wrongdoers.

Malaysia has comprehensive regulatory measures that compel financial institutions to ensure consumer protection from financial fraud and related risks. In terms of preventive regulatory measures, the BNM countermeasures, which are a set of mandatory actions imposed by BNM on all financial institutions since 2022, are implemented to protect consumers. For instance, requirements include limits on the number of registered devices linked to a single user that can be used to perform banking transactions[94] .

Beyond this, we observe that financial institutions are working on innovative measures to protect victims from frauds and scams. The National Addressing Database (NAD) by PayNet is one of them. The NAD is a centralised repository that stores mappings between DuitNow IDs (which can be a mobile phone number, NRIC, passport number, or business registration number) and the designated bank accounts or e-wallets linked to those identifiers. When an individual initiates a DuitNow Transfer using a DuitNow ID, the recipient's registered name is displayed before the transaction is authorised. This enables the payer to verify the intended recipient before transferring funds[95].

Importantly, the NAD also enhances traceability. By maintaining mappings between DuitNow IDs and their linked accounts, it enables participating financial institutions to identify the account associated with a particular DuitNow ID for payment processing and, where legally authorised, to support investigations and law enforcement efforts to trace account holders.

As cyber risks are increasing over time, insurance agencies have introduced personal cyber fraud insurance for consumers, enabling them to insure themselves against online risks, including scams. Previously, cyber fraud insurance was only provided to businesses and organisations. Now, these insurance policies for personal coverage have also been increasingly popular in Malaysia. Some existing plans are Z-Alliance Cyber Protect, Pacific Personal Cyber Insurance and GXBank and Zurich Malaysia Cyber Fraud Protect, which cover financial loss due to different kinds of cyber incidents such as cyber financial fraud, online retail fraud, and e-commerce purchase protection.

Gaps

From the above, we observe no significant gaps for the laws and policies, however **efforts are deemed too reactive.** According to stakeholders in the financial sector, Malaysia is sufficiently

[94] BNM (2025a)
[95] PayNet (n.d.)

covered by finance-related laws. Existing laws and countermeasures adopted by banks and other financial institutions already provide extensive coverage for consumers, and compel banks to take various measures to protect consumer assets, be it information or money. Both the Financial Services Act (FSA) and Islamic Financial Services Act (IFSA) allow for coordination of tracing funds across the financial ecosystem through BNM when transactions are deemed suspicious. However, stakeholders have suggested a need for more proactive measures beyond laws and policies[96] such as using big data analytics to inform early warning systems.

Cyber fraud insurance still in its infancy: According to the study "Adoption of Cyber Insurance in Malaysian Organisations" by Rahman et al. (2022), cyber insurance within Malaysia is considered to be in its infancy stage even at an organisational level. Authors of the study claim that this is a result of "limited cyber insurance coverage options due to the lack of standardised cyber risk assessment and potential misunderstanding between an insurer and an insured"[97]. The regulation of cyber fraud insurance is not as comprehensive as other insurance types in Malaysia due to its nascency, a gap that should be filled so that consumers' online activities can be adequately insured[98] .

3.6. Disappearing Act

Core issue: Law enforcement

Key actors: PDRM, NACSA, ASPs

At this stage, the scammer obscures their trails as to go undetected by authorities trying to trace them after obtaining the funds. The key issue here is to track down the scammer from their digital and physical trails through law enforcement. Often, this process requires close collaboration among law enforcement, platforms and cybersecurity professionals. The effectiveness of law enforcement is hampered by issues below:

Proper and timely reporting from victim faces barriers: According to NSRC, the first 24 hours are crucial for reporting so that financial institutions can intercept any stolen funds and for police to begin their investigations [99]. However, in Malaysia, there appears to be significant barriers for reporting financial scams. In the 2025 State of Scams in Malaysia report, 23% of scam victims surveyed did not report the incident. Top reasons include being unsure who to report to (35%) and believing that their report would not make a difference (34%)[100].

[96] Stakeholder interviews
[97] Rahman et al. (2022)
[98] Stakeholder Interview
[99] National Scam Response Centre (2025)
[100] Global Anti-Scam Alliance (2025)

Mule accounts complicate tracking processes: In most of the cases, the proceeds of scam are transferred across a network of mule accounts, instead of being sent directly to the mastermind's account. According to the Home Ministry, a total of 218,307 accounts were detected to involved in scam-related activities from 2023 to 2025[101]. The breakdown by year shows that between 2024 and 2025, there had been a 70% increase in the number of accounts identified. Scammers either dupe the account owners, pay them money between RM200 to RM500 per account, or promise them a monthly income to allow usage of their accounts. Usually, vulnerable groups strapped for cash such as students, retirees, low-income workers, and job seekers are targeted for these schemes[102].

Regulatory measures and non-regulatory measures in place

Existing regulatory laws and policy provisions include the guidelines developed for financial reporting institutions and law enforcement authorities.

The Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA) stipulates, in its First Schedule, the requirement for reporting institutions[103] to comply with measures aimed at preventing money laundering. As part of enforcement efforts, to tackle the misuse of mule account, Section 424A to 424D of the Penal Code apply.

Malaysia has also deepened its engagement with international enforcement bodies through accession to, or participation in, international conventions such as the Budapest Convention on Cybercrime and the United Nations Convention against Cybercrime. This collaboration extends to areas such as joint investigations, the exchange of digital evidence, and the extradition of cybercriminals. For more details of the regulatory measures, see Appendix 7.

Non-regulatory measures for this stage cover two main types. The first includes initiatives and tools developed to support law enforcement behind the scenes, usually used by respective stakeholders in the financial and cybercrime systems. Examples include, at the national level, the NAD, the NFP and the National Financial Crime Intelligence System (NFIS); while at the international level there are Project Frontier+ and Operation First.

The second type includes public-facing measures that help users verify information while also serving as a database for law enforcement authorities to keep records of fraudulent or mule accounts, fake identities, and numbers implicated in fraudulent activities. The NSRC 24-hour hotline and PDRM CCID Semak Mule platform are such examples.

Appendix 8 provides a detailed list of non-regulatory measures.

---

[101] The Vibes (2026)
[102] Singh (2025)
[103] Such as financial institutions, law firms and accounting firms

Gaps

Increasing strain on law enforcement officers: Scam cases are becoming increasingly rampant, as evidenced by the statistics presented in Table 2. While the surge in reported cases may be attributed to various factors, such as increased public awareness of reporting or the use of more sophisticated technology in enabling scams, it should be noted that the continued rise in total cases may overwhelm law enforcement authorities in the long run if no sustainable solutions are implemented.

Inadequate international coordination: There is an uneven adoption of anti-money laundering (AML) laws and regulations across different jurisdictions. While many countries have adopted AML standards, the implementation of these standards is inconsistent and is relatively weak in certain countries, creating jurisdictional ambiguity. This creates "safe havens" for criminals and hinder the effectiveness of the legal processes[104]. This creates cross-jurisdictional issues once the transaction crosses borders. While projects such as the Project FRONTIER+ and Operation First Light provide avenues for overcoming this challenge, issues such as conflicts, political sensitivities, elite protection, and weak governance in countries like Myanmar, Cambodia, Laos and Thailand continue to fuel scam syndicates[105].

3.7. Cashing Out

Core issue: Money laundering

Key actors: BNM, PDRM, NFCC, SC, MACC and financial institutions

Money laundering is not a new challenge for the Malaysian financial system, but increasing sophistication of virtual assets such as cryptocurrencies and non-fungible tokens have diversified methods for scammers to conceal the illegal source of their money. As mentioned in Section 2.2, this usually works by moving funds away from the original source in a layered fashion with the goal of extracting money from the financial system and then reintroducing it in a legitimate form.

While recognizing that numerous methods exist to execute money laundering including purchasing assets, establishing shell companies and making stock investments, this discussion paper mainly addresses two persistent tactics that scammers use to extract the money, that is through Automated Teller Machine (ATM) withdrawals and cryptocurrency exchanges.

ATM used for cash withdrawals: Many scam syndicates have been found to cash out illegal funds via multiple mule accounts, enabling the money to escape tracing by regulators. Based on previous PDRM operations, scammers purchase ATM cards from members of the public or obtain

[104] Beh (2025)
[105] Surachanee Sriyai (2025)

ATM cards as collaterals from victims of scams[106]. They may target low-income individuals to provide access to their bank accounts to be used as mule accounts in exchange for money. Furthermore, criminals running scam syndicates hire "runners" to withdraw the money at the ATMs instead of going there themselves. Scammers provide salaries for runners, even up to RM3,500 per month, and send instructions via messaging channels such as Telegram. The runners are then asked to send the money to specified addresses through delivery services[107]. This enables them to remain anonymous, as enforcement authorities would only be able to identify the runners through existing measures such as tracking individual activity via CCTV at ATM machines.

Cryptocurrency used to mask money trail: While cryptocurrencies are not recognised as legal tender in Malaysia, they are accepted as securities, meaning that they are tradeable and to some extent regulated by the SC. Stakeholders note that the difficulty in tracking cryptocurrency transactions contributes to scams due to the "anonymous and immutable nature" of blockchain technology[108]. While public coins use pseudonyms (wallet addresses are publicly available), privacy coins use Privacy Enhanced Technologies (PETs) to further obscure transactions such as by using decoys through ring signatures and stealth addresses[109]. This offers further anonymity when conducting cryptocurrency transactions, making it difficult for law enforcement agencies to trace stolen funds. Certain methods of transaction also add to this, such as by using mixers, or multi-input-multi-output (MIMO) which makes tracing transactions difficult[110].

By using "smart contracts"[111], decentralised exchanges (DEXs) enable users to have disintermediated access to financial services which allows them to make cryptoasset-to-cryptoasset exchanges in real time. These DEXs lack a central administrator with active oversight of user accounts, records, identities or activities, and ultimately allows users to escape tracing from law enforcers. Combined with foreign digital asset exchanges (DAXs), which allows buying, selling and trading of cryptocurrencies without Malaysian regulation, scammers can be virtually anonymous in their transactions.

Low restitution success rates: The success rates of tracing, recovering and returning funds to victims remain unsatisfactory. In January 2026 alone, NSRC received 19, 438 scam-related calls. The Ministry of Home Affairs reported that RM 2.408 billion was intercepted and frozen before further transfers were made. However, only RM321.3 million has been successfully returned to victims, which constitutes about 13% of the total funds frozen[112].

[106] Noh (2024)
[107] Noor (2025)
[108] Ibid.
[109] Chainalysis (2023)
[110] Sammis Law Firm (2026)
[111] Automatic execution of transactions when predefined conditions are met. Liu et al. (2024)
[112] The Vibes (2026)

Regulatory measures and non-regulatory measures in place

The Cashing Out stage is governed primarily by the Second Schedule of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA) in Malaysia. It empowers law enforcement and regulatory agencies to conduct money laundering investigations and prosecute wrongdoers accordingly. Assets believed to be involved in money laundering may also be forfeited under this legislation.

In addition, regulatory measures such as Financial Action Task Force (FATF) compliance requirements and the Securities Commission Malaysia's Guidelines on Digital Assets set forth standards and obligations that must be adhered to by relevant institutions in their respective areas, namely, combating money laundering and regulating cryptocurrency activities.

See Appendix 9 for more details on the regulatory measures.

In most of the cases, cracking down on money laundering, especially in the digital space, is a complicated process that requires cross-agency cooperation. An example of such an endeavour is the expansion of the Inland Revenue Board of Malaysia (LHDN)'s tax evasion operations to digital currency-related activities. Through the "Ops Token" operation, LHDN, with the help from PDRM and CSM, tracked the evasion of gains from cryptocurrency transactions[113]. Seen in the context of our paper, this is equivalent to cracking down on money laundering schemes through cryptocurrency platforms.

Gaps

Measures in terms of laws and policies are well-developed and have extensive coverage to deal with money laundering offences. In addition, they are constantly being updated by the relevant institutions based on international evaluation and recommendations.

According to players within the financial sector, there is satisfactory coordination between financial institutions and enforcement agencies in Malaysia, such as PayNet, BNM and PDRM[114]. There are dedicated teams within each organisation working on tackling cyber financial crimes[115]. However, despite strong laws and good cross-organisational collaboration, certain aspects can be improved.

Inability to regulate or monitor decentralised crypto exchanges and privacy coins: PETs and DEXs use sophisticated technology to evade detection and tracing, and obtain enhanced anonymity rather than just pseudonymity of regular cryptocurrency practices. Blockchain

[113] LHDN (2024)
[114] From stakeholder interviews
[115] Stakeholder interview

analytics companies have made notable progress in tracking suspicious activity, however it is found that privacy coins and mixing protocols continue to outpace detection tools[116].

Unidentifiable ATM cash withdrawals: ATM withdrawals remain a common way for scammers to remove the money from traceable systems, and also implicate other individuals to cover up their tracks. The main issue comes from the fact that scammers are able to withdraw money using ATM cards even though the registered owner of those cards are not present at the time of withdrawal, especially in situations where Personal Identification Numbers (PINs) have been compromised.

Wrongly targeted mule accounts: The issue of false positives is concerning, as it may adversely affect innocent individuals who are wrongly flagged as mule account holders. Once flagged as a mule, an individual's bank account may be immediately frozen, and rectifying the matter through the Sessions Court can take a significant amount of time. This situation places unnecessary stress on innocent individuals, particularly those who have a limited number of savings accounts in use[117].

Data collected by the FOMCA show a similar finding: most affected consumers who unknowingly become involved in mule activities have to wait at least one to three months for their frozen accounts to be reinstated or cleared by the authorities. In some cases, the process may extend beyond three months, particularly when multiple agencies are involved or when the banks concerned fail to provide sufficient updates[118].

[116] Wilson, Williams, and Taylor (2025)
[117] Stakeholder interviews
[118] FOMCA (2025)

4. Recommendations

In this section, we present some overarching observations, followed by specific recommendations for Malaysia. These are synthesised from a systematic review of existing measures and gaps discussed in the previous section, combined with findings from our desk research and data collection.

4.1. Overarching Observations

We begin with some high-level observations that serve to frame the policy recommendations that follow. These are not ordered by importance and are intertwined in nature.

Firstly, **a plethora of regulations exist across the scam lifecycle**, which makes sense as scams are not a new phenomenon and regulatory frameworks have been put in place to protect consumers over the years. These are generally sufficient as a foundation and should be updated in specific and strategic ways to adapt to technological advancements and rapid adoption by malicious actors. Over-regulation should be avoided to ensure regulatory coherence and effectiveness.

Secondly, **Malaysia's regulatory initiatives are more mature within the financial and investigative areas, which are towards the tail end of the Scam Anatomy**. The crux of the matter lies in the reactive nature of the solutions, highlighting that more work is needed to strengthen proactive prevention. This situation is not unique to Malaysia. During the roundtable co-organised by KRI and Columbia University, Professor Jungpil Hahn presented the case of Singapore, arguing that initiatives tackling AI-enabled financial scams are disproportionately focused on the end stage of financial extraction when victims' funds are already lost. Earlier stages where technology is used to lay the groundwork for deception and targeting of victims receive less emphasis.

Thirdly, **much of the focus on preventative measures are on digital and financial literacy campaigns**, which are extensively conducted by multiple parties (see Section 3.4 and Appendix 6 for details). Despite the efforts, the unrelenting rise of cyber financial scams points to two imperatives: the need to improve the effectiveness of these campaigns, and the need to extend beyond literacy campaigns for proactive prevention.

Fourthly and relatedly, **policy interventions need to consider the entire scam lifecycle to distribute the risk and responsibility beyond the individual**. The strong focus on digital and financial literacy indicates that the current logic puts the onus on the individual user or consumer to protect themselves. However, as shown in the Scam Anatomy, there are multiple actors and issues involved as the scam progresses from preparatory work to cashing out. As technology advances, it gets increasingly untenable and unfair to expect individuals to keep pace with technology-enabled risks and shoulder all the responsibility of keeping themselves and their communities safe.

Fifthly, **government and industry actors are racing to contain cyber financial scams, especially on the technological front.** During the writing of this paper, there have been rapid

developments in regulatory frameworks to plug gaps upstream in the earlier stages of the Scam Anatomy. This includes the Risk Mitigation Code under ONSA 2025 that came into force in June 2026, covering AI content labelling and also compelling ASPs and CASPs to verify the identities of advertisers. Earlier in the year, big tech companies such as Meta also released new features and pledges to combat online scams. We note and encourage these, as social media platforms and other application service providers have thus far been the weakest link in the Scam Anatomy chain.

As we operate in an increasingly dynamic environment, all stakeholders must remain mindful that the threat landscape is constantly shifting, and the recommendations provided below are reactions to a particular snapshot in time. The rise of new technologies and associated threats, such as in the case of quantum computing and agentic AI, will bring forth new risks that will need to be addressed at a later point.

4.2. Policy Recommendations

The recommendations that follow do not aim to be exhaustive. We focus on aspects that we find to be most pressing, mainly on the systemic and gaps due to technological advances.

Distributing risk and responsibility among key enabling actors

In Malaysia's current landscape, scam-related risk and responsibility are mostly placed on the individual even though many institutional actors play a role in preventing or enabling the occurrence of scams throughout the scam lifecycle.

We advocate for **an equitable distribution of risks and responsibilities among enabling actors along the scam lifecycle**, including ASPs and CASPs, telecommunication companies, and financial institutions. Ideas can be drawn from other countries such as Taiwan and Singapore which have progressive frameworks in place to achieve this (see Box 3).

Box 3: Distributing risks and responsibilities: Cases of Taiwan and Singapore

Distributing risks and responsibilities: Cases of Taiwan and Singapore

Taiwan - Fraud Crime Hazard Prevention Act

Passed in 2024, the Act recognises scams not as isolated criminal incidents, but as outcomes of a complicated ecosystem of enabling infrastructure and actors. Three layers are taken into account: 1) online platforms and digital advertising systems, 2) telecommunications infrastructure and 3) payment and financial systems. From there, the Act proceeds to allocate anti-fraud obligations and responsibilities to actors within these systems, with a safe harbour principle of exempting liability to businesses if they act in accordance with their preventative obligations.

Singapore - Shared Responsibility Framework (SRF)

Jointly developed by the Monetary Authority of Singapore (MAS) and the Infocomm Media Development Authority (IMDA), the SRF serves as a clear set of guidelines to clarify the allocation of responsibility for losses arising from scams. The SRF's "waterfall approach" distributes the burden equitably amongst financial institutions, telecommunications companies and victims in phishing scams.

Financial institutions will be held accountable first as "custodians of consumers' money" if they fail to discharge their duties. Next would be the telecommunication companies, which would need to facilitate SMS delivery for digital payments. Should both financial institutions and telecommunications companies fulfil their duties accordingly, the victim will bear full financial loss for the scam. However, if either one or both of the institutions are found to be negligible in discharging their duties, they will bear the full loss and are required to compensate the consumer.

Taiwan tackles the problem from a duty-based and preventative angle, while Singapore attempts to attribute the burden of losses fairly to bolster the impact of scams on individuals. Another point to note is that Taiwan's model addresses digital and online platforms, while Singapore's does not. While these two countries differ somewhat in approach, the spirit of what is accomplished is similar. Risks and responsibilities are shifted to institutional actors who are better placed structurally to prevent and weather losses coming from cyber financial scams.

We recommend that Malaysia considers this shift in paradigm and tailors an approach suitable for its regulatory and institutional environment, with an emphasis on proactive and systemic prevention. While the BNM has a framework, the Policy Document on Ensuring Fair Treatment for Victims of Unauthorised e-Banking Transactions (SEFT), to compel banks to compensate customers when financial loss is caused by the bank's security gaps, SEFT applies only to cases involving unauthorised transactions[119]. In other words, SEFT does not apply to scam cases where

[119] Bank Negara Malaysia (2024)

victims are manipulated into willingly initiating and approving transactions (see our definition of cyber financial scams in Section 2.1).

Integrating technological solutions with existing legal and information systems

As explored in Section 3, Malaysia has many regulatory and non-regulatory initiatives in place to combat scams along the scam lifecycle. For example, ONSA 2025 provides the legal means to take down scam content; and platforms such as PDRM's Semak Mule exist to help consumers and organisations verify and authenticate information. However, these mechanisms and tools are often not connected in a systemic manner or within a meaningful workflow to increase their utility. **Technological solutions designed to connect and build upon existing legal and information systems will increase their effectiveness.**

Firstly, to address scam advertisement on online platforms in tandem with the enforcement of ONSA, we suggest the development of **a scam advertisement detection tool that can be used together with ONSA for efficient takedowns.**

A case study is the online fraud reporting and inquiry platform released by Taiwan's Ministry of Digital Affairs, which has been attributed for the success in reducing scam ads from a weekly rate of 77,000 down to below 900. The tool uses a combination of Natural Language Processing (NLP) and big data analytics to conduct round-the-clock scanning, detection and escalation of scam ads to relevant platforms for takedown. At the same time, it allows consumers to report and escalate ads missed by the tool. The efficient and timely detection of scam ads feeds into Taiwan's Anti-Fraud Initiative's work to take down content via the Fraud Crime Hazard Prevention Act. Malaysia can use a similar workflow, to automate scam ad detection and use that in conjunction with the ONSA, which imposes a statutory deadline on online platforms to verify and remove fraudulent advertisements upon notification.

Secondly, we suggest the development of **a dedicated scam prevention application that integrates with existing official databases and tools** to serve as a single source of truth for consumers. The following are some of the proposed features that can draw on existing datasets identified:

- Opt-in functions for short message service (SMS) and call blocking: By leveraging the Number Verification API (see Section 3.2), the application can verify a mobile user's identity by authenticating the phone number against real-time network data. Where a phone number is identified as suspicious, the application (subject to the user's prior consent) can automatically block SMS messages and calls from reaching the user, thereby preventing the initial point of contact between scammers and potential victims.
- The use of AI-powered chat functions including uploading pictures and files for verification: Agencies such as MCMC receive incident reports of scam and fraudulent content, and this data can be used to train a user-facing AI chatbot, so that users would be able to verify information and content that they suspect to be scam-related. The chatbot can also guide users on how to respond to scam incidents and update them about emerging trends.

- Consolidation of all the authentication and verification tools available: The application can consolidate and draw from the numerous databases available to consumers, such as PDRM's Semak Mule Platform, BNM's Financial Consumer Alert List, SC's Investor Alert List, and so on (See Table 9 in Appendix 6 for more details) to provide a one-stop shop for consumers to verify information.

Given that such an approach would likely require users to share their personal data, robust safeguards for data privacy and security must be established and maintained before the application is rolled out to the public. Where resources are allocated for the development of such an application, the government must ensure its long-term sustainability and continuous maintenance. This can be achieved by appointing a lead agency to oversee, operate, and maintain the application.

There are also existing apps that can be built upon to serve the above functions. An example is Scamora, developed by Leogics Solutions in collaboration with NFCC, which already has some of the suggested features in its beta phase, such as chatbots and consolidation of verification tools. It can be scaled up, integrating more innovative features to serve as a robust scam prevention tool – potentially even serving as a data collection point for predictive analytics when there is a critical mass of users.

Providing accurate, timely and publicly available data for scam monitoring

Malaysia lacks a consolidated, authoritative and publicly viewable platform for scam data. We encourage **the establishment of a public dashboard on scam statistics** to fill this gap. The dashboard should serve as a central repository for key statistics such as the number of scam reports received (disaggregated by scam type), total financial losses reported, demographic breakdowns of scam types, and variations in loss amounts across demographic groups.

An example of publicly available scam data at a national level is Australia's Scamwatch, developed by Australia's National Anti-Scam Centre. It provides transparent and up-to-date scam data, offering comprehensive insights, including top 10 scam types, gender and geography breakdowns, top contact methods, and so on.

As it stands, data on scams in Malaysia is available in a piecemeal fashion, released during press conferences and parliamentary speeches for instance. Discrepancies are occasionally observed between different sources. As an example, the PDRM reported that 208,000 mule account holders were identified in 2024, whereas in 2025, the KDN stated in Parliament that 173,224 mule accounts were identified between 2022 and July 2025.

A public-facing dashboard is important for several reasons.

First, data within the dashboard would provide a transparent baseline for year-on-year comparisons. Numbers over time would track broader trends and provide a comprehensive picture of the trajectory of scam activities. Establishing a single source of truth across different actors in this landscape is also important to avoid discrepancies that may lead to inconsistent

responses or misaligned priorities among stakeholders. In addition, key agencies will be able to avoid doing double work in collecting similar types of data.

Second, the clear presentation of scam statistics can provide valuable indicators of the most pressing scam types affecting the public, across dimensions such as demographics, geography, and channels of occurrence. Insights drawn would enable authorities and frontline responders (including CSOs) to better identify and focus resources on communities more vulnerable. Linking back to our previous recommendation on evidence-based literacy campaigns, the available data allows for more targeted and tailored interventions, ultimately improving scam prevention outcomes.

Third, transparent reporting of the total number of scam cases nationwide may help increase vigilance among the public, and improve reporting rates. Publicly available scam statistics may reduce stigma and shame associated with being a scam victim. From a psychological perspective, victims may feel less embarrassed and less reluctant to lodge reports with the authorities.

At this juncture, it is important to recognise that a high rate of incident reporting is critical to ensure that authorities have accurate data that reflect realities on the ground. Efforts therefore need to be channelled into encouraging prompt reporting, perhaps by increasing public confidence in the authorities' capabilities to handle incidents.

Enhancing literacy campaigns to build anti-scam resilience

Multiple digital and financial literacy initiatives are already available (see Section 3.4 and Appendix 6), mainly providing information about scams and scam types. As scams evolve to be more complex, awareness initiatives need to move beyond providing basic information on scam identification. Digital hygiene practices and fact-checking habits need to be instilled as a matter of instinct, and there should be a distinct focus on effective response when faced with suspicious situations as well as post-scam.

There is therefore need to **update anti-scam campaigns to be more evidence-based, engaging and innovative** to build a scam-resilient population. Some examples of how this can be achieved are:

- Evidence-based digital and financial literacy modules: To achieve widespread and sustainable behavioural change, stakeholders running literacy programmes need to delve deeper into the psychology of scams and environmental factors that enable them. In other words, thoughtful literacy modules should investigate the root causes of successful scams, and effective ways to defend against them, before embarking on a communication campaign. Programmes tailored to specific communities will be more effective than generic information packs. Campaigners can also draw insights from fields like behavioural science to design interventions for better outcomes[120].

[120] Emilie and Bergmann (2025)

- Simulation training[121]: An example of a simulated scam experience was provided during our Roundtable, where an MCCA representative invited participants to scan a QR code for alleged security check on their phone. Participants who scanned the QR code later found out that a selfie photo was taken without their consent or knowledge and transferred to the representative's phone. Such drills are engaging and can leave a strong impression, to fortify the public in understanding experientially how scams work. Further training can guide them on how they should best respond.
- Scam awareness sandboxes[122]: Innovation labs or sandboxes can provide a space to incubate and test innovative ideas to increase scam awareness and response capabilities. Innovators can receive monetary and non-monetary support to test different methods and tools to raise public awareness on evolving scam tactics and operations.

In general, content on scam awareness needs to be constantly updated to keep up with the evolving nature of scams. This, combined with the need to tailor content to the target audience and to ensure that messaging is aligned, points to the need for more streamlined coordination across the board among stakeholders who are working on digital and financial literacy. This coordination will also reduce overlaps in work and enable better use of resources to increase the quality of campaigns.

Closing legal gaps and enacting forward-looking legislation

Malaysia's regulatory frameworks are generally adequate in the area of cyber financial scams, especially in the financial sector. Interventions should be strategically targeted at gaps yet unfilled.

For instance, while we generally view the increased uptake of cyber fraud insurance among Malaysians as potentially enhancing consumer protection, we recommend that the government first **examine the regulatory framework governing cyber fraud insurance**. As a relatively new form of insurance in the country, regulatory oversight is necessary to protect consumers from unfair practices and to ensure that policy terms are reasonable and transparent. This is essential for building consumer confidence in adopting cyber fraud insurance for its benefits.

The legal landscape in Malaysia is shifting rapidly to match the speed of technological advancement. During the writing of this paper, ONSA 2025 was fortified by accompanying subsidiary legislation, codes and guidelines such as the Risk Mitigation Code, and the Cybercrime Bill was passed in parliament. There are ongoing legislations that are being drafted and amended, such as the AI Governance Bill and the Electronic Commerce Act (2006), potentially including specific provisions that will help in protecting consumers from scams. We suggest expediting and prioritising these provisions, including but not limited to:

[121] Example provided by the MCCA in the stakeholder interview
[122] Example provided by the MCCA in the stakeholder interview

- **Online Dispute Resolution (ODR) system:** An ODR system should be developed to allow for more effective and timely management of disputes in the e-commerce context, particularly those involving fraud[123].
- **Updated industry-wide standard list of controlled and prohibited items on E-Commerce Platforms:** Greater regulatory authority should be conferred upon the Ministry of Domestic Trade and Cost of Living (KPDN) to enhance its enforcement capabilities over e-commerce platforms. Specifically, this should include stricter regulation of platforms regarding the sale of controlled and prohibited goods, with the list to be regularly updated. Importantly, pre-registered prepaid SIM cards should be among the first additions to this list.

Forward-looking legislation is crucial to ensure that Malaysia remains ahead of the curve. As emerging technological threats continue to evolve, the government must **consistently monitor trends and develop preventive measures, rather than responding reactively.** To remain adaptable, tech-related laws should be subject to periodic review to be responsive to the changing technological landscape.

Enhancing law enforcement capacity and safeguards

As cyber financial scams rapidly expand, we recommend **increasing resources for law enforcement agencies to strengthen their technical capacity and communications,** at the same time, putting in place **safeguards to mitigate unintended consequences arising from more comprehensive enforcement.**

As pointed out by the KDN, shortages in technical expertise and human resources within cyber enforcement teams and digital forensics are major hurdles in the country's fight against financial scam syndicates. In particular, the use of emerging technologies in scams has outpaced the capabilities of officers in handling such cases. Considering the growing volume of scam cases, this underscores the need for greater support and expertise to proactively and efficiently tackle scam syndicates. In addition, it is telling that a significant proportion of scam victims choose not to lodge police reports as they believe that it does not make a difference (see Section 3.6). More resources therefore need to be allocated to law enforcement on upskilling and communications at the grassroots level.

As more resources are invested in strengthening enforcement, it is equally important to recognise that some unintended consequences may arise from tight enforcement. The case of wrongly targeted mule accounts in Stage 7 (Cashing Out), for instance, illustrates how misdirected enforcement can seriously disrupt the lives of innocent individuals. While robust enforcement is encouraged, authorities should be mindful of such effects and have proper mitigation plans in place.

[123] Qirana Nabilla Mohd Rashidi (2026)

In this specific context, we recommend the government expedite the handling of false-positive cases involving mule account freezing, to ensure that the lives and livelihoods of innocent individuals are not unduly disrupted. Especially for those with limited access to alternative funds, the wait for court processes to reinstate access to their accounts causes undeserved stress. Through acting proactively, public confidence in enforcement agencies will also be strengthened.

Strengthening cybersecurity defence

Data breaches provide the intelligence for background research and targeting of victims (see Section 3.1). Cybersecurity safeguarding data security therefore serves as frontline defence, raising the difficulty for scammers to operate effectively.

As mentioned in gaps identified in Stage 1 (Foundation Work), there is currently a shortage of approximately 10,000 cybersecurity professionals in the country by NACSA's estimates. Basic digital security in businesses and agencies is generally lacking, leaving data and systems vulnerable to cyberattacks and fuelling scam operations. Hence, we encourage stakeholders to invest, nurture and develop **more talent in the cybersecurity field** as a matter of priority**.**

Additionally, both public and private entities are encouraged to provide sufficient budgetary allocations to train non-cybersecurity personnel on basic cybersecurity measures relevant to their job functions, ensuring that sensitive data and the integrity of systems are preserved.

5. Conclusion

The rapid digitalisation of our communication and financial services have brought about much efficiency and convenience. At the same time, improved productivity and seamlessness have also enabled malicious actors to scale up the volume and speed of cyber financial scams. To continue reaping the benefits of technology, it is a matter of putting in adequate safeguards and incident responses to mitigate risks that come with it.

As scams remain to be a lucrative business and a serious threat, proactive and preventative measures need to be put in place to anticipate evolving challenges as they come. Reactive responses are no longer excusable considering the sophistication of operation and the scale of harm.

A key lesson from the Scam Anatomy is that scams should not be viewed in a piecemeal manner. Each stage in the scam lifecycle presents distinct entry points that scammers can exploit to execute their schemes. A whole-of-system approach is therefore required, with all stakeholders working in concert to address vulnerabilities at every level.

In analysing regulatory and non-regulatory initiatives in Malaysia, we note that many mechanisms have been put in place to combat scams. Yet, efforts need to move from defence at the individual level to structural prevention and duty of care. In this regard, shared responsibility and distributed risk is essential and remains a central principle underpinning our recommendations.

It is our hope that this paper contributes meaningfully to ongoing efforts to combat cyber financial scams.

6. Appendices

Appendix 1: Roundtable Participants List

Topic : Roundtable Discussion: Best Practices for Regulatory Approaches to AI-Deepfakes Used in Financial Scams
Date : 20 November 2025
Venue : Khazanah Research Institute

No.	Organisation	Name	Designation
Malaysian Participants			
1	Bank Negara Malaysia (BNM)	Mr. Muhamad Fahim Aqil bin Muhamad Sahlan	Technological Risk Analyst
2	Bar Council	Ms. Sarah Yong	Chair of the Cyber & Privacy Laws Committee
3	Khazanah Research Institute (KRI)	Prof. Dr. Jomo Kwame Sundaram	Research Advisor
4	Khazanah Research Institute (KRI)	Dr. Jun-E Tan	Senior Research Associate
5	Legal Affairs Division of Prime Minister's Department (BHEUU)	Mr. Thiyagu Ganesan	Deputy Director-General
6	Legal Affairs Division of Prime Minister's Department (BHEUU)	Ms. Amirah Fatimah binti Salahul Ahamed	Administrative Officer
7	Malaysia Cyber Consumer Association (MCCA)	Mr. Mohamad Sirajuddin bin Jalil	President
8	Malaysian Communications and Multimedia Commission (MCMC)	Mr. Saiful Azhar Johari	Head of Content Moderation Department
9	Malaysian Communications and Multimedia Commission (MCMC)	Mr. Zahid Ahmad	Deputy Director, Content Moderation Department
10	National AI Office Malaysia (NAIO)	Mr. Darmain A/L Vijaya Segaran	Manager
11	National Anti-Financial Crime Centre (NFCC)	Ts. Dr. Mohamad Nizam bin Kassim	Deputy Director
12	PayNet	Ts. Dr. Endry Lim	Chief of Staff
13	Royal Malaysia Police (PDRM)	ACP Tay Kim Chuan	Head of CCID, Negeri Sembilan

14	Royal Malaysia Police (PDRM)	Insp. Ganesh Raman	Investigation Officer
Overseas Participants			
15	Australia eSafety Commissioner	Ms. Sarah Fox	Australia Manager International Engagement
16	Australia Institute's Democracy & Accountability Program	Mr. Bill Browne	Director
17	Australian High Commission	Ms. Kate Wienke	First Secretary (Political Economic)
18	Columbia University	Dr. Anya Schiffrin	Senior Lecturer
19	Columbia University	Prof. Dr. Joseph E. Stiglitz	Professor
20	Columbia University	Ms. Navya Sinha	Student
21	Ministry of Communication and Digital Affairs (Indonesia)	Ms. Mediodecci Lustarini	Executive Secretary of the Directorate General of Digital Space Monitoring
22	National University of Singapore, AI Singapore	Prof. Dr. Jungpil Hahn	Provost's Chair Professor
23	Taiwan's National Institute of Cyber Security (NICS)	Dr. Mattel Hsu	Vice President

Appendix 2: Application of the Scam Anatomy – The Case of Online Romance Scam

Table 4: Online romance scam process following the anatomy of cyber financial scam

Stages	Scam Process
Foundation Work	The romance scam operation starts with the formation of an organised group. Within the scam group, the scammers would undergo training to equip themselves with skills to pull off the romance scam. The scammers then hunt for the potential target(s) to engage with. The target selection is usually conducted in few ways – looking for individuals with certain characteristics (e.g. rich, divorced), or using a "scattergun approach" (mass targeting). Information about the targets is also gathered (sometimes involving data theft or data purchasing) during this stage.
Operational Setup	An array of items including a false persona with a backstory, associated documentation and a fake digital profile are fabricated to support the scam operation.
Establishment of Contact	After the preparation, the scammers make the move to establish initial contact with the targets. In some cases, the targets unwittingly make the first move through channels like dating apps or social media. After the contact, scammers usually attempt to shift the conversation to a private channel to isolate the target and avoid monitoring by platforms.
Luring, Baiting and the Ask	Using the backstory developed prior to contact, the scammers start the grooming phase to foster trust and build emotional commitment between both parties. Sending gifts, video-calling, exchanging intimate photos and "love bombing"[124] are some of the typical techniques used. When enough trust is garnered, the scammers transition into requesting for money. In most cases, this is a gradual process, with a "foot in the door" technique where smaller amounts of money will first be requested before asking for a larger sum of money. A story of crisis is provided to create an urgent situation (such as a sick relative), to mount pressure on the victim into giving out his or her money. In the case of resistance or doubt, emotional manipulation (inducing guilt, self-harm threats, physical harm threats, silent treatment etc.) is used to suppress resistance and strengthen obedience.
'Hurrah' Moment	By escalating scenarios, the victim is finally convinced to hand out a significantly large amount of money to the scammer. The transfer of money can be made in various ways – bank transfers, money transfer via money transfer operators (MTO)[125], cryptocurrency, gift cards or even through a fake app or platform built by scammers.

[124] Manipulative tactic to overwhelm one through excessive attention and affection over a short period of time.

[125] Service providers that offer money transfer services to individuals or businesses.

Disappearing Act & The Loop	At this point, the scammers will either "ghost" victims by going missing entirely, or in the case of being exposed, the victim may end the relationship on their own. Alternatively, scammers may choose to deploy revictimisation, looping back to earlier phases (Operational Setup, or Luring and Baiting) when the victim stops giving out money. Some of the revictimisation strategies include scammer admitting the scam but pretend to have developed genuine feelings towards the victims. Once the victim falls into this "authentic relationship" trap, the scammer will engage in another round of the romance scam. In another common revictimisation tactic known as "recovery scam", the scammer plays the role as a third party striving to recover the lost money on behalf of the victim, pretending that he or she has nothing to do with the money lost. Once such illusion is bought by the victim, similar to the above, another round of scamming will follow. When the scam has been successfully carried out, the victim will be added to the "sucker lists" to enable other scammers to gain the victim information, allowing them to target the "easy prey". The scam comes to its definitive end when all revictimisation attempts fail.
Cashing Out	Money laundering practices is usually done after receiving the payments from the victims.

Source: Adapted from Schokkenbroek and Snaphaan (2025).

Appendix 3: Regulatory Measures in Place – Foundation Work

To safeguard data privacy and security, Malaysia has a number of laws as part of its regulatory framework, the details of which are summarised in Table 5.

Table 5: Malaysian laws related to data privacy and security

Act	Description
Computer Crimes Act 1997 (CCA)	Enacted to criminalise the misuse of computers, the CCA deals with offences such as malware attacks and hacking. For instance, unauthorized access to computer materials and unauthorized modification of computer content are deemed unlawful and punishable under the Act.
Personal Data Protection Act 2010 (Amendment 2024) (PDPA)	Focusing on the protection of personal data in commercial transactions in Malaysia, the PDPA only applies to the private sector. Specifically, it spells out the responsibilities and duties that must be upheld by the data controller and data processors, guided by key principles such as the disclosure principle and security principle. Mandatory data breach notifications were introduced in the amendment in 2024.
Cyber Security Act 2024 (CSA)	As a public-sector facing law with the goal of enhancing national cyber defences, the CSA protects the cybersecurity of National Critical Information Infrastructure (NCII)[126]. This includes mandating codes of practice set out by NCII sector leads, cyber security risk assessments, audits as well as timely and mandatory cyber security incident reporting. Additionally, in alignment with this act, NACSA has developed MyKriptografi, a national policy framework that determines the government direction for cryptographic governance, research and application. It serves as the national architect of the 'Digital Shield,' protecting against sophisticated cyber threats that extend into the quantum computing era[127].
Communications and Multimedia Act 1998 (Amendment 2025) (CMA)	The CMA was first introduced in 1998 and amended in 2025 to strengthen online safety and minimise network security risks. The amendment expands the power of MCMC in a new chapter on network security, complementing the CSA 2024 on defining the role of MCMC as the NCII sector lead for 'Information, communication and digital'. Specifically, it gives power to the MCMC to instruct any person to take appropriate measures or comply with requirements which are deemed necessary to prevent, detect or counter any network security risk.

[126] a computer or computer system which the disruption to or destruction of the computer or computer system would have a detrimental impact on the delivery of any service essential to the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the ability of the Federal Government or any of the State Governments to carry out its functions effectively.

[127] For more info regarding the framework, read https://www.nacsa.gov.my/kriptografi.php

Appendix 4: Non-Regulatory Measures in Place – Foundation Work

Since its establishment, CyberSecurity Malaysia has introduced a number of initiatives and efforts under the pillars of Awareness, Identify and Detect, Manage and Protect, Respond and Recover, Government and Compliance to safeguard the cyber ecosystem in Malaysia[128]. Some of the key initiatives are as below:

Table 6: Key initiatives of CyberSecurity Malaysia (non-exhaustive list)

Initiative	Description
Cyber Security Awareness for Everyone (CyberSAFE®) Program	On the non-regulatory front, CyberSAFE® Program is a dedicated program designed to educate and increase public awareness on cybersecurity issues, aiming to create a safe online space for the Malaysian public. One of the key efforts is through 'CyberSAFE® untuk Rakyat' that covers modules such as cybersecurity, personal data protection, cybersafety, Wi-Fi threats, mobile devices security and so on.
CYBER999 Cyber Incident Response Centre	Cyber999 serves as the point of contact at the national level for the general public to report computer security incidents through different means such as an online form, email, hotline and the Cyber999 mobile app. Following the reporting of an incident, it aims to guide the affected users on the ways to respond to and resolve such incidents. Beyond that, Cyber999 publishes Incident Statistics on a monthly basis and issues alerts and advisories to raise public awareness on latest cybersecurity threats or incidents. Lastly, together with Computer Security Incident Response Team, Cyber999 facilitates the improvement on computer security incident response capability for organisations.
Cybersecurity Competency & Certification Training (CyberGuru)	CyberGuru provides a platform that offers a list of competency-based training programmes and certifications to nurture information security practitioners and enhance the development of cybersecurity professional. The levels of training courses range from fundamental and intermediate to specialisation and professional certification.
Mobile Assessment Security Scanning Application (MASSA)	MASSA, a mobile application designed for only Android users, is a security tool that provides security scanning on end users' devices to detect any risks of potential malicious activity posed by downloaded applications or software in the smartphone.

[128] For a detailed list of the services provided, visit https://www.cybersecurity.my/

Appendix 5: Regulatory Measures in Place – Operational Setup

Table 7: Laws covering issues on authentication and verification

Act	Description
Online Safety Act 2025 (ONSA)	The ONSA was enacted to safeguard the online environment, particularly through the regulation of harmful content and the imposition of duties and obligations on CASPs and ASPs. Specifically, "content on financial fraud" is part of the listed "priority harmful content" of the Act, subjected to additional and prioritised controls. The CASPs and ASPs have the responsibility to 1) mitigate risk of exposure to harmful content, 2) provide sufficient tools and settings on their services to prevent or limit other users from identifying, locating or communicating with harmful content and 3) establishing mechanism that makes priority harmful content inaccessible to all users.
Communications and Multimedia Act 1998 (Amendment 2025) (CMA)	The CMA is the foundational legislation that led to the establishment of MCMC. The CMA has an extensive coverage of areas, primarily revolving around regulatory, licensing, and enforcement power of the MCMC within Malaysia's communications and multimedia industry. The act was later amended in 2025. Below are some of the key provisions in the CMA related to the Operational Setup stage. **Social media licensing** Effective 1 January 2025, MCMC mandated that all social media services and internet messaging service providers with 8 million or more users in the country would need to apply for the Application Service Provider Class License (ASP (C) License), to prevent online harm and improve regulatory oversight. As compliance to this was uneven, starting from 1 January 2026, platforms fulfilling the criteria were deemed automatically registered. This is an important step to address regulatory gaps. By categorising these platforms as licensees, they are lawfully subjected to statutory provisions, licence conditions and regulatory directions issued by the MCMC, where enforcement actions can be taken under the CMA as well as the ONSA.

Commission Determination on the Mandatory Standards for the Registration of End-Users of Prepaid Public Cellular Services, Determination No.1 of 2026[129]	MCMC has released its revised mandatory standards for the registration of prepaid public cellular service users, to replace the previous Guidelines on Registration of End-users of Prepaid Public Cellular Services 2017, enforced starting 26 February 2026. Intended as a "decisive regulatory step" to curb fraudulent activities, some key measures introduced include: **Verification of prepaid SIM Card user through biometric authentication and MyDigital ID** To register for a new prepaid line, Malaysians now have to verify their identity through either biometric authentication (fingerprint) or MyDigital ID. Assisted registration (such as through a retail seller) requires biometric authentication while self-registration requires e-verification through MyDigital ID, performed exclusively on the official authorised platform provided by the telecommunication service provider. The same process is required in the event of SIM card replacement. The biometric authentication requirement also applies to non-Malaysians where a passport reader that comes with biometric authentication (facial recognition) will be used to verify foreign end-users. **Limit on the number of prepaid SIM card and service validity for non-Malaysians** For non-Malaysians, the mandatory standard puts a cap of two SIM cards per service provider on each individual, a significant tightening compared to the previous limit of five. In addition, prepaid services registered by tourists have a maximum validity period of three months.

[129] MCMC (2026b)

Appendix 6: Non-Regulatory Measures in Place – Luring, Baiting and the Ask

Table 8: Ongoing awareness campaigns on scams

Starting Year	Awareness Campaign	Main Stakeholders	Description
2026	Online Safety IRL[130]	Ministry of Communications, CelcomDigi, Meta Platforms, Inc., Tonton, Ratio: Cause	A 3-months fellowship that nurture creators and youths into advocates for online safety.
2025	Kempen Internet Selamat[131]	Ministry of Communication, MCMC	A series of national-level initiatives from 2025 to 2027 that aim to enhance public awareness and strengthen the capability of Malaysians in addressing cybersecurity challenges.
2025	HATI-HATI, SCAMMER TIDAK MENGENAL LELAH![132]	NFCC, Dewan Bandaraya Kuala Lumpur	A one-off financial crime prevention program and online scam awareness campaign targeted at the public.
2023	Kempen #JanganKenaScam[133]	The Association of Banks in Malaysia, Association of Islamic Banking and Financial Institutions Malaysia, BNM	A national scam awareness campaign launched and carried out by the banking industry.
2023	Jelajah Anti-Scam Kebangsaan[134]	CSM, CelcomDigi, Gabungan Bertindak Anti-Scam (GBAS), PDRM, MCMC etc.	The national anti-scam townhalls that are held in different states of Malaysia to provide education and awareness to the consumers regarding scam activities.
2020	Financial Education Network (FEN)[135]	Inter-Agency Grouping co-chaired by BNM and SC, with members including MoE, MoHE, Perbadanan Insurans Deposit Malaysia, Employees Provident Fund, Agensi Kaunseling dan Pengurusan Kredit and	An inter-agency platform established to drive efforts in promoting effective delivery of financial education initiatives to Malaysians.

130 https://www.onlinesafetyirl.com/

131 Https://www.mkn.gov.my/web/ms/2025/11/03/kempen-internet-selamat-perkasa-literasi-digital-negara/

132 NFCC (2025)

133 https://www.jangankenascam.com/my/

134 CelcomDigi (2023)

135 https://www.fenetwork.my/

		Permodalan Nasional Berhad.	
2020	Amaran Scam[136]	BNM	A Facebook page dedicated to updating trending financial scam activities in Malaysia.
2014	InvestSmart®[137]	SC	The SC's investor education initiative to educate the public on investment-related topics through various initiatives.
2012	Klik Dengan Bijak[138]	MCMC	Internet safety initiative focusing on target groups such as children, teenagers, parents, guardians, and adults.

Table 9: Tools for authentication and verification

Tools	Stakeholders	Description
Semak Mule CCID Platform[139]	CCID	Official platform of the PDRM that allows individual to check bank account, phone number or company that are suspected to be related to scam cases.
Financial Consumer Alert List[140]	BNM	A guide for consumers to check if an entity or a financial scheme is licensed or regulated by BNM.
Investor Alert List[141]	SC	A detailed list for consumers to check the particulars of unauthorised entities and individuals.
Licensed Financial institutions List[142]	BNM	A directory that enables the consumers to check if a financial institution is licensed.
i-KreditKom[143]	Ministry of Housing and Local Government	An application for the Malaysian public to verify licensed money lending companies.
Sebenarnya.my[144]	MCMC	A platform established by MCMC to help Malaysians verify information online. Users can submit a verification request via an online form, and officers check the facts before verifying the authenticity of the information.

[136] https://www.facebook.com/amaranpenipuan/
[137] https://investsmartsc.my/
[138] https://klikdenganbijak.my/en/index
[139] https://semakmule.rmp.gov.my
[140] https://www.bnm.gov.my/financial-consumer-alert-list
[141] https://www.sc.com.my/investor-alert-list
[142] https://www.bnm.gov.my/regulations/fsp-directory
[143] https://play.google.com/store/apps/details?id=my.gov.onegovappstore.iKrediKom&pcampaignid=
[144] https://sebenarnya.my/

MyCheck Malaysia[145]	BERNAMA	An independent platform established by BERNAMA to help Malaysians verify information online. Users can submit a verification request via an online form, and officers check the facts before verifying the authenticity of the information.

Table 10: List of digital literacy and financial literacy interventions

Intervention	Description
Digital literacy interventions in the education system	The MoE has taken over the CyberSAFE programme in schools (formerly run by the CSM) since 2025. Some key programs that are include National ICT Security Discourse (NICTSeD), an annual debate competition amongst secondary school students about ICT security issues[146]. The CSM continues as a technical partner to provide updates, technical training and digital curriculum support to teacher trainers, and monitoring and evaluation of implementation. It also maintains a website that provides videos, quizzes, games and information on cybersecurity for kids, youths, parents and organisations. MoE collaborated with the Ministry of Digital (KD) to develop a National Cyber Ethics Module under CyberSAFE. It was expected to be fully deployed in schools starting January 2026. Topics that were announced to be in the module include Digital Fluency, Digital Ethics, Digital Health and Well-being, Digital Commerce, Digital Privacy and Security, and Digital Rights and Responsibilities[147].
Financial literacy interventions in the education system	Kurikulum Standard Sekolah Rendah/Menengah (KSSR/KSSM) introduced cross-curricular elements in all of the subjects taught in national schools. One of these elements is 'financial education'. According to guidelines set by MoE, these elements can either be taught directly with dedicated topics such as 'Money' in Mathematics that teaches simple and compounding interests or inserted into other topics appropriately. To increase teachers' financial literacy and better integrate financial education in their lessons, the Financial Education Network worked with Financial Industry Collective Outreach, to conduct teachers' training-of-the-trainer style workshops under Program Latihan Kejurulatihan Pengurusan Kewangan Peribadi Guru, with sponsorship and support from financial institutions and an e-commerce platform. Post-workshop, organisers provided monetary support for teachers to train other teachers in their respective districts. One topic is specifically dedicated to 'investments and scams', referring to classification of assets, and spotting fake investments, based on information from the SC. The subsequent topic is on 'digital financial literacy', which covers digital scams, how digital literacy and financial literacy are interconnected, and ways to stay safe online. Teachers also gain access to existing financial literacy programs run by the sponsors, allowing them to bring these programs to their schools according to suitability.

[145] https://www.mycheck.my/
[146] CyberSecurity Malaysia (2023)
[147] Kementerian Digital (2025)

Appendix 7: Regulatory Measures in Place – Disappearing Act

Table 11: Existing laws in incident reporting and tracing scammers

Intervention	Description
Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA)	The act outlines strict obligations for reporting institutions, including entities such as financial institutions, law firms and accounting firms. These are requirements imposed on financial reporting institutions to implement a risk-based approach and enhanced customer due diligence with regard to any transactions – including conducting risk profiling, monitoring transactions and profile updates. Mandating STRs regardless of transaction amount enables close monitoring and tracing of individuals and entities involved in illegal activities such as scams.
Penal Code (Amendment 2024)	Section 424A to 424D of the Penal Code are introduced, as part of the amendment in 2024, specifically to address the use of mule accounts, curb account-rental schemes and prevent the misuse of third-party financial information.
Budapest Convention on Cybercrime United Nations Convention against Cybercrime	As of September 2025, Malaysia is in the process of joining the Budapest Convention on Cybercrime and has been officially invited to accede. Malaysia is currently an observer to the Convention. Meanwhile, in October 2025, Malaysia has also become a signatory to the United Nations Convention Against Cybercrime. By signing these treaties, it paves way for deeper collaboration between Malaysia and international enforcement bodies in areas such as joint investigations, digital evidence exchange, and cybercriminal extradition.

Appendix 8: Non-Regulatory Measures in Place – Disappearing Act

Table 12: Existing non-regulatory measures supporting law enforcement and intelligence gathering

Intervention	Description
National Addressing Database	PayNet developed the NAD, a centralised system to store the details of all the DuitNow IDs and their linked identifiers, bank accounts and e-wallets. Financial institutions utilising DuitNow can access these IDs to trace the identities of DuitNow accounts. This effort supports the enforcement, investigations and tracing of account owners.
National Fraud Portal	The NFP is the coordination portal for all financial institutions in Malaysia to freeze assets, block transactions, trace accounts in the case of financial scams. It uses machine learning to flag mule accounts, classifying accounts based on previous cases. It has a high precision rate due to its network view and "across the board" enforcement where each participating institution needs to adhere to the same rules in blacklisting accounts implicated as mules. This enables financial institutions to more efficiently stop mule accounts and trace the identity of the main scammer[148].
National Financial Crime Intelligence System (NFIS)	The NFIS is a centralised data information system set up, administered and maintained by NFCC to help with the joint investigation process across government entities and other law enforcement agencies by compiling and sharing data when needed for prosecution.
Project FRONTIER+ (Funds Recovery Operations & Networks Team, Inspiring Effective Resolution Plus)	This project is a cross-border scam operation between NSRC with 10 other jurisdictions within the Asia-Pacific region since October 2024. The unified front has since successfully taken down a number of transnational scam syndicates[149].
Operation First Light	Malaysia, through ASEANAPOL, participated in a global police operation, Operation First Light in 2024, coordinated by INTERPOL to combat online scams. It was a successful operation: up to 6,745 bank accounts were frozen, hundreds of millions worth of assets being seized, and thousands of suspects were arrested. The main system used was INTERPOL's Global Rapid Intervention of Payments, or better known as I-GRIP. It is a stop-payment mechanism that helps member countries trace and intercept criminal proceeds. that stem largely from cyber-enabled fraud – in the form of fiat and cryptocurrency[150].
NSRC 24-hour (997) hotline	Serves to connect victim to financial institutions and law enforcement services in a timely manner to freeze assets and trace the transactions to find implicated accounts.

[148] Stakeholder interview
[149] SPF Insider (2025)
[150] Interpol (2024)

	**Since September 2025, as PDRM took the lead at the NSRC, a call to the 997 hotline is now equivalent to lodging a police report. Hence, there is no need for victim to make another police report on top of calling the NSRC hotline.*
PDRM CCID Semak Mule Platform	This publicly available database provides access to a consolidated repository of numbers and accounts that have been implicated in fraudulent transactions for banks and law enforcement forces to trace suspicious accounts to determine fraudulent transactions.

Appendix 9: Regulatory Measures in Place – Cashing Out

Table 13: Regulatory measures in place to combat money laundering

Intervention	Description
Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLATFPUAA)	This is the primary legislation in Malaysia to prevent, detect and prosecute money laundering and terrorism financing. The act empowers the authorities to freeze and forfeit illicit assets.
Financial Action Task Force (FTAF) Compliance	The FATF is an intergovernmental organisation that sets global standards for combating money laundering and terrorism financing that have to be followed by forty member countries including Malaysia. The task force issues “black” and “grey” lists to identify high-risk jurisdictions and publishes country-specific comprehensive reporting on AML/ Countering Financing of Terrorism (CFT) regime effectiveness.
Guidelines on Digital Assets from the SC on Cryptocurrency	Key requirements set forth by the SC to regulate cryptocurrencies as a form of securities that rest on three pillars: investor protection, market integrity and responsible innovation.

7. References

Abdul Hamid, Haezreena Begum. 2025. "SIM Card Scams Are Not Due to Our Carelessness." *Malaysia Gazette*, November 2025. https://malaysiagazette.com/2025/11/13/sim-card-scams-are-not-due-to-our-carelessness/.

Alafaa, Princess U. 2022. "Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World." *Available at SSRN 4005750*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4005750.

Alias, Izzarafiq. 2026. "Experts: SIM Card Misuse Fuelled by Weak Regulation." The Star. February 6, 2026. https://www.thestar.com.my/news/nation/2026/02/06/experts-sim-card-misuse-fuelled-by-weak-regulation.

Ambashtha, Kanahaiya Lal, and Pramod Kumar. 2023. "Online Fraud." In *Financial Crimes: A Guide to Financial Exploitation in a Digital Age*, 97–108. Cham: Springer International Publishing.

Arthur State Bank. n.d. "Fraud and Scams — What They Are and How They Differ." https://www.arthurstatebank.com/blog/fraud-and-scams-what-they-are-and-how-they-differ/.

Atan, Mohd Amirul, Ahmad Azfar Abdul Hamid, Sheik Badrul HishamJamil Azhar, Nuramirah Zaini, and Nur Aqilah Norwahi. 2025. "Language, Technology, and Policy: A Unified Conceptual Framework for Combating Digital Scams in Malaysia." *International Journal of Research and Innovation in Social Science* IX (IX):1003–9. https://doi.org/10.47772/IJRISS.2025.90900088.

Bank Negara Malaysia. 2024. "Ensuring Fair Treatment for Victims of Unauthorised E-Banking Transactions." https://bnm.gov.my/documents/20124/938039/Ensuring_Fair_Treatment_for_Victims_of_Unauthorised_eBanking-Transactions.pdf?_gl=1*k2t4a6*_ga*MjEwNTkwMzA5NS4xNzY1MzU1MzM2*_ga_QCXBYX5C31*czE3NzY4NDQwNDQkbzEzJGcxJHQxNzc2ODQ0NDI5JGo1NyRsMCRoMA.

Bassett, Gabriel, C. David Hylender, Philippe Langlois, Alexandre Pinto, and Suzanne Widup. 2020. "Verizon 2020 Data Breach Investigations Report."

Beh, May Ting. 2025. "Combating Scam Syndicates in Malaysia and Southeast Asia," March 19, 2025. https://penanginstitute.org/publications/issues/combating-scam-syndicates-in-malaysia-and-southeast-asia/.

BERNAMA. 2025. "Police Detect Five Deepfake Videos Linked To Investment Scam." BERNAMA. December 3, 2025. https://bernama.com/en/news.php?id=2401443.

———. 2026. "MCMC Receives 203,918 Takedown Requests, 91 Per Cent Related To Gambling, Scams – Fahmi." April 20, 2026. https://www.bernama.com/en/news.php?id=2547037.

BERNAMA TV. 2025. *Cybersecurity: Malaysia Faces 10,000 Skilled Worker Shortage*. https://www.youtube.com/watch?v=pu17Cl69pV4.

BNM. 2024. “Financial Capability and Inclusion Demand Side Survey 2014.” Bank Negara Malaysia. https://www.bnm.gov.my/documents/20124/17493532/ar2024_en_box4.pdf.

———. 2025a. “Annual Report 2024.” Bank Negara Malaysia. https://www.bnm.gov.my/documents/20124/17493532/ar2024_en_box7.pdf.

———. 2025b. “Assistant Governor’s Keynote Address at the PayNet Engagement Forum 2025 - Bank Negara Malaysia.” October 2025. https://www.bnm.gov.my/-/agne-pef2025.

———. n.d. “Money Laundering & Terrorism Financing.” Anti-Money Laundering & Counter Financing of Terrorism Malaysia. Bank Negara Malaysia. https://amlcft.bnm.gov.my/what-is-money-laundering.

Butts, and Renee. 2024. “Psychological Manipulation.” EBSCO. 2024. https://www.ebsco.com.

CelcomDigi. 2023. “Jelajah Anti-Scam Kebangsaan Sasar Tingkatkan Pengetahuan Dan Kesedaran Mengenai Jenayah Penipuan Dalam Talian.” 2023. https://corporate.celcomdigi.com/news/jelajah-anti-scam-kebangsaan-sasar-tingkatkan-pengetahuan-dan-kesedaran-mengenai-jenayah-penipuan-dalam-talian.

———. 2024. “CelcomDigi National Scam Awareness Survey 2024 Report.” https://cdn.prod.website-files.com/639b20bcbc27667faa23c543/6694bffb9e02d8f651047b97_CelcomDigi%20National%20Scam%20Awareness_Survery_2024_Report_2024.pdf.

Chainalysis. 2023. “Privacy Coins 101: Anonymity-Enhanced Cryptocurrencies.” April 18, 2023. https://www.chainalysis.com/blog/privacy-coins-anonymity-enhanced-cryptocurrencies/.

Chandraiah, Jagadeesh, Pankaj Kohli, Xinran Wu, and Szabolcs Lévai. n.d. “Fake Android and iOS Apps Disguise as Trading and Cryptocurrency Apps.” Sophos. https://www.sophos.com/blog/fake-android-and-ios-apps-disguise-as-trading-and-cryptocurrency-apps.

Consumer Protection Team. n.d. “Website Spoofing - Scammers Disguised as Trusted Brand.” https://www.michigan.gov/consumerprotection/protect-yourself/consumer-alerts/business/website-spoofing.

Corrons, Luis. 2025. “How Social Media Fuels Scams: Trends, Tactics, and Best Practices.” GASA. May 22, 2025. https://www.gasa.org/post/how-social-media-fuels-scams-trends-tactics-and-best-practices.

CyberSecurity Malaysia. 2023. “A Decade of NICTSeD.” https://www.cybersafe.my/nictsed/download/A_Decade_of_NICTSeD-8x8in-v4e-highres.pdf.

Department of Statistics Malaysia. 2025. “ICT USE AND ACCESS BY INDIVIDUALS AND HOUSEHOLDS SURVEY REPORT 2024.”

dev@thebrandonagency.com. 2024. “Fraud vs. Scams: What’s the Difference?” *Arthur State Bank* (blog). June 21, 2024. https://www.arthurstatebank.com/blog/fraud-and-scams-what-they-are-and-how-they-differ/.

Emilie, Buttarelli, and Jessica Bergmann. 2025. “Integrating Behavioural Science into Education.” UNICEF. 2025. https://www.unicef.org/innocenti/media/10376/file/UNICEF-Innocenti-DMS-Method-Brief-BehaviouralScience-2025.pdf.

Estrella, Rosanina. 2021. “Scam Design: The Anatomy of Online Products & Services Scams.” Te Herenga Waka-Victoria University of Wellington. https://doi.org/10.26686/wgtn.16600259.

EUROPOL. n.d. “Economic Crime.” https://www.europol.europa.eu/crime-areas/economic-crime.

Fam, Christopher. 2025. “Telcos to Combat Fraud, Digital Identity Theft with Federated Network Service.” The Star. September 23, 2025. https://www.thestar.com.my/tech/tech-news/2025/09/23/telcos-to-combat-fraud-digital-identity-theft-with-federated-network-service.

FMT. 2026a. “RM5.62bil Lost to Online Scams in 3 Years.” January 21, 2026. https://www.freemalaysiatoday.com/category/nation/2026/01/21/rm5-62bil-lost-to-online-scams-since-2023.

———. 2026b. “Online Crime Cases Nearly Double in 2025, Resulting in RM3bil Losses.” February 23, 2026. https://www.freemalaysiatoday.com/category/nation/2026/02/24/online-crime-cases-nearly-double-in-2025-resulting-in-rm3bil-in-losses.

FOMCA. 2025. “Mule Accounts Reveal Deep Fault Lines in Banking.” Federation Of Malaysian Consumers Associations. 2025. https://www.fomca.org.my/v1/index.php/fomca-di-pentas-media/fomca-di-pentas-media-2025/2018-mule-accounts-reveal-deep-fault-lines-in-banking.

“Fraud and Scams | How To Spot The Difference – HSBC UK.” n.d. Accessed December 18, 2025. https://www.hsbc.co.uk/help/security-centre/fraud-guide/difference-between-fraud-and-scams/.

“Fraud vs. Scams: How to Spot the Difference and Stay Safe.” n.d. Accessed December 18, 2025. https://b2b.mastercard.com/news-and-insights/blog/fraud-vs-scams-how-to-spot-the-difference-and-stay-safe/.

Global Anti-Scam Alliance. 2025. “State of Scams Malaysia 2025.” https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_2ce49273719f4aa7a6e42f4f05550a99.pdf.

Global Anti-Scam Org. 2025. “The Hidden World of SIM Card Agents: A Lucrative Side Hustle or a Gateway to Crime?” March 7, 2025. https://www.globalantiscam.org/post/the-asean-sim-card-market-a-key-enabler-of-online-scam-centers.

Hao, Wei. 2025. “Half the Spam in Your Inbox Is Generated by AI – Its Use in Advanced Attacks Is at an Earlier Stage.” Barrcuda Blog. June 18, 2025. https://blog.barracuda.com/2025/06/18/half-spam-inbox-ai-generated.

Hasham, Salim, Shoan Joshi, and Daniel Mikkelsen. 2019. “Financial Crime and Fraud in the Age of Cybersecurity.” *McKinsey & Company* 2019:1–11.

Hooper, Joe, Bill Bannear, and Gary Chew. 2025. *Anti-Scam Handbook v2.0: Collective Response and Tools to Safeguard Development*. 2.0. UNDP Global Centre for Technology, Innovation and Sustainable Development. https://www.undp.org/sites/g/files/zskgke326/files/2025-05/undp_anti-scam_handbook_v2.0.pdf.

Horwitz, Jeff. 2025. "Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show." *Reuters*, November 6, 2025, sec. Investigations. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

HSBC UK. n.d. "Fraud and Scams." https://www.hsbc.co.uk/help/security-centre/fraud-guide/difference-between-fraud-and-scams/.

Information Technology Industry Council. 2024. "Authenticating AI-Generated Content - Exploring Risks, Techniques & Policy Recommendations." https://www.itic.org/policy/ITI_AIContentAuthorizationPolicy_122123.pdf.

Institute for Strategic Dialogue. 2025. "The Trust-Consensus Paradox: Why Decentralized Fact-Checking Faces Challenges on Polarizing Topics." 2025. https://www.isdglobal.org/digital-dispatch/the-trust-consensus-paradox-why-decentralized-fact-checking-faces-challenges-on-polarizing-topics/.

Interpol. 2024. "USD 257 Million Seized in Global Police Crackdown against Online Scams." 2024. https://www.interpol.int/News-and-Events/News/2024/USD-257-million-seized-in-global-police-crackdown-against-online-scams.

Izuakor, Dr Christine. 2019. "How Cyber Attackers Hide Their Tracks After Committing Digital Fraud?" *Veriato* (blog). November 19, 2019. https://veriato.com/blog/how-cyber-attackers-hide-their-tracks-after-committing-digital-fraud/.

Jassmine Shadiqe. 2025. "Scripted Deception: How Scammers 'coached' Doctor into RM8.7mil Loss." *Business Times*, August 4, 2025. https://www.nst.com.my/news/crime-courts/2025/08/1254952/scripted-deception-how-scammers-coached-doctor-rm87mil-loss-watch.

Kaspersky. 2019. "What Is Cybercrime and How to Protect Yourself?" AO Kaspersky Lab. November 6, 2019. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime.

———. 2020. "What Is Social Engineering?" August 26, 2020. https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering.

Kementerian Digital. 2025. "Modul Etika Siber Nasional Di Sekolah Seluruh Negara Akan Dilancarkan Pada Jan 2026." November 25, 2025. https://www.digital.gov.my/siaran/Modul-Etika-Siber-Nasional-Di-Sekolah-Seluruh-Negara-Akan-Dilancarkan-Pada-Jan-2026.

Kontorskyy, Denys. 2024. "Outlook Spam Filter Explained [2026]." Mailtrap. January 13, 2024. https://mailtrap.io/blog/outlook-spam-filter/.

Kumaran, Neil. 2022. "An Overview of Gmail's Spam Filters." Google Workspace. Google. 2022. https://workspace.google.com/blog/identity-and-security/an-overview-of-gmails-spam-filters.

Kunkel, Matt. 2025. “Frictionless Payments Are a Fraud Factory. Banks Can’t Afford the Tab.” The Financial Brand. September 22, 2025. https://thefinancialbrand.com/news/payments-trends/frictionless-payments-are-a-fraud-factory-banks-cant-afford-to-keep-picking-up-the-tab-192416.

Lexis Nexis. n.d. “Three Stages of Money Laundering: An In-Depth Guide & Prevention.” https://www.lexisnexis.com/en-gb/glossary/money-laundering-stages.

LHDN. 2024. “Kenyataan Media Perluasan Asas Cukai Terus Diperkasa Menerusi Operasi Pematuhan Khas ‘Ops Token’.Pdf.” 2024. https://www.hasil.gov.my/media/f0vfbzv3/20240615-kenyataan-media-hasil-perluasan-asas-cukai-terus-diperkasa-menerusi-operasi-pematuhan-khas-ops-token.pdf.

Liu, Yang, Jinlong He, Xiangyang Li, Jingwen Chen, Xinlei Liu, Song Peng, Haohao Cao, and Yaoqi Wang. 2024. “An Overview of Blockchain Smart Contract Execution Mechanism.” *Journal of Industrial Information Integration* 41. Elsevier:100674.

LSEG Risk Intelligence. n.d. “Layering in AML: Hiding Illicit Transactions.” https://www.lseg.com/en/risk-intelligence/glossary/aml/layering.

MalayMail. 2026. “Romance Gone Rogue: Malaysians Lose RM3.5m to Love Scams in Jan, Mostly Victims Aged 30 to 50, Says Bukit Aman | Malay Mail.” February 22, 2026. https://www.malaymail.com/news/malaysia/2026/02/22/romance-gone-rogue-malaysians-lose-rm35m-to-love-scams-in-jan-mostly-victims-aged-30-to-50-says-bukit-aman/209994.

Malaysian Bar. 2025. “Press Statement | Rebuilding the Public Trust Deficit With Regard to Personal Data Collection - The Malaysian Bar.” June 2025. https://www.malaysianbar.org.my/article/news/press-statements/press-statements/press-statement-rebuilding-the-public-trust-deficit-with-regard-to-personal-data-collection?utm_source=chatgpt.com.

Marchand, Cory. 2025. “The Psychology of Social Engineering.” Coalition. February 2025. https://www.coalitioninc.com/blog/security-labs/the-psychology-of-social-engineering.

Mastercard. n.d. “Fraud vs. Scams: How to Spot the Difference and Stay Safe.” https://b2b.mastercard.com/news-and-insights/blog/fraud-vs-scams-how-to-spot-the-difference-and-stay-safe/.

Maurer, David. 2010. *The Big Con: The Story of the Confidence Man*. Anchor.

Maybank. n.d. “Sim Card Replacement Scam.” Security Alert. https://www.maybank2u.com.my/maybank2u/malaysia/en/personal/security_alert/simcard_replacement_scam.page.

MCMC. 2023. “Licensing Guidebook.” https://mcmc.gov.my/skmmgovmy/media/General/pdf2/Suruhanjaya-Komunikasi-dan-Multimedia-Malaysia_Licensing-Guidelines.pdf?utm_source=chatgpt.com.

———. 2024. “Over 10,000 Websites Blocked by MCMC since 2022.” August 2024. https://mcmc.bernama.com/news.php?id=2327059.

———. 2026a. “Public Inquiry Report on Commission Determination on the Mandatory Standards for the Registration of End-Users of Prepaid Public Cellular Services.” https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/Public-Inquiry-Report-on-the-New-Commission-Determination-on-the-Mandatory-Standards.pdf.

———. 2026b. “Commission Determination on the Mandatory Standards for the Registration of End-Users of Prepaid Public Cellular Services Determination No.1 of 2026.” February 2026. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/Commission-Determination-on-the-Mandatory-Standards-for-the-Registration-of-End-Users-of-Prepaid-Public-Cellular-Services-26022026.pdf.

Meta Newsroom. 2026. “Meta Launches New Anti-Scam Tools, Deploys AI Technology to Fight Scammers and Protect People.” March 11, 2026. https://about.fb.com/news/2026/03/meta-launches-new-anti-scam-tools-deploys-ai-technology-to-fight-scammers-and-protect-people/.

Mouton, Francois, Mercia M. Malan, Louise Leenen, and H.S. Venter. 2014. “Social Engineering Attack Framework.” In *2014 Information Security for South Africa*, 1–9. https://doi.org/10.1109/ISSA.2014.6950510.

MyCERT. 2026. “Cyber Incident Quarterly Summary Report - Q3 2025.” CyberSecurity Malaysia. https://www.mycert.org.my/portal/advisory?id=SR-032.012026.

National Institute of Standards and Technology. n.d. “Authentication.” NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/authentication.

National Scam Response Centre. 2025. “NSRC FAQs.” Laman Web Rasmi Pusat Pencegahan Jenayah Kewangan Nasional (NFCC). February 6, 2025. https://nfcc.jpm.gov.my/index.php/en/about-nsrc.

NFCC. 2025. “Program Pencegahan Jenayah Kewangan Dan Kempen Kesedaran Mengenai Penipuan Dalam Talian (Online Scam) : HATI-HATI, SCAMMER TIDAK MENGENAL LELAH!” January 2025. https://nfcc.jpm.gov.my/index.php/en/aktiviti/program-pencegahan-jenayah-kewangan-dan-kempen-kesedaran-mengenai-penipuan-dalam-talian-online-scam-hati-hati-scammer-tidak-mengenal-lelah.

Nik Faiz Nik Ruzman. 2025. “Malaysia Faces Urgent Need to Address Cybersecurity Skills Gap, According to Fortinet’s SEA Senior Director.” Cyber Security Asia. February 24, 2025. https://cybersecurityasia.net/malaysia-cybersecurity-skills-gap-fortinet/.

Noh, Norzamira Che. 2024. “16 People Arrested in Syndicate Selling Bank Accounts, ATM Cards.” NST Online. March 29, 2024. https://www.nst.com.my/news/crime-courts/2024/03/1031999/16-people-arrested-syndicate-selling-bank-accounts-atm-cards.

Noor, Hafidzul Hilmi Mohd. 2025. “Lima ‘runner’ Sindiket along Ditahan Bersama 2,924 Kad ATM Peminjam.” Harian Metro. August 18, 2025. https://www.hmetro.com.my/mutakhir/2025/08/1253606/lima-runner-sindiket-along-ditahan-bersama-2924-kad-atm-peminjam.

Norris, Gareth, Alexandra Brookes, and David Dowell. 2019. “The Psychology of Internet Fraud Victimisation: A Systematic Review.” *Journal of Police and Criminal Psychology* 34 (3):231–45. https://doi.org/10.1007/s11896-019-09334-5.

Nurqalby Mohd Reda. 2023. “Don’t Let Your Guard Down Against Online Fraud, Experts Warn.” BERNAMA Fokus. December 29, 2023. https://www.bernama.com/en/bfokus/news.php?current&id=2258037.

Ong, Charmayne, Jillian Chia, and Natalie Lim. n.d. “Malaysia to Introduce Comprehensive Legal Framework for Artificial Intelligence.” Skrine - Advocates & Solicitors. http://www.skrine.com/insights/alerts/december-2025/malaysia-to-introduce-comprehensive-legal-framewor.

PayNet. n.d. “PayNet APIs Documentation - National Addressing Database.” https://docs.paynet.my/docs/national-addressing-database/overview.

Petty, Richard, and John Cacioppo. 1986. “The Elaboration Likelihood Model of Persuasion.” *Advances in Hydroscience* 19 (July):124–205.

Qirana Nabilla Mohd Rashidi. 2026. “Online Dispute Resolution Launched to Tackle E-Commerce Fraud.” The Sun. February 5, 2026. https://thesun.my/news/malaysia-news/people-issues/online-dispute-resolution-launched-to-tackle-e-commerce-fraud/.

Rahman, Nur Hidayah Abd, Rajeswari Raju, Suriyani Ariffin, Nor Hasnul Azirah Abdul Hamid, and Atif Ahmad. 2022. “Adoption of Cyber Insurance in Malaysian Organisations.” *International Journal of Innovative Computing* 12 (2):45–51. https://doi.org/10.11113/ijic.v12n2.380.

RinggitPlus. 2024. “Malaysian Financial Literacy Survey 2024.” https://ringgitplus.com/en/blog/wp-content/uploads/2024/09/RMFLS-2024-Survey-Report.pdf.

Rosenorn-Lanng, Emily. 2019. “Cyber Fraud and Scamming.” *National Centre for Post-Qualifying Social Work*. https://proceduresonline.com/trixcms2/media/1377/cyber-fraud-and-scamming-ecopy-2.pdf.

Sammis Law Firm. 2026. “Common Tracing Cryptocurrency Problems and Mistakes.” Criminal Defense Attorney Tampa. February 11, 2026. https://criminaldefenseattorneytampa.com/asset-seizure-asset-forfeiture/cryptocurrency/tracing/.

SC. 2025. “SC and MCMC To Combat Scams Via Enhanced Regulatory Oversight,” January 3, 2025. https://www.sc.com.my/resources/media/media-release/sc-and-mcmc-to-combat-scams-via-enhanced-regulatory-oversight.

Securities Commission. 2024a. “Guidance Note on Provision of Investment Advice.” https://www.sc.com.my/api/documentms/download.ashx?id=d22c8909-06e8-40bf-a8da-4fc31b4606c0.

———. 2024b. “SC Cautions Public on Investment Scams Using Fake Information Memorandums - Media Releases | Securities Commission Malaysia.” 2024. https://www.sc.com.my/resources/media/media-release/sc-cautions-public-on-investment-scams-using-fake-information-memorandums.

Shang, Yuxi, Kaijie Wang, Yuye Tian, Yingyu Zhou, Beibei Ma, and Sanyang Liu. 2023. “Theoretical Basis and Occurrence of Internet Fraud Victimisation: Based on Two Systems in Decision-

Making and Reasoning." *Frontiers in Psychology* 14 (February):1087463. https://doi.org/10.3389/fpsyg.2023.1087463.

Singh, Habhajan. 2025. "Mules Make the Scam Machine Go." *The Malaysian Reserve*, September 22, 2025, sec. News. https://themalaysianreserve.com/2025/09/22/mules-make-the-scam-machine-go/.

Snow, Jackie. 2025. "Cybercriminals Use AI to Create Fake Websites That Look Just Like the Real Thing." *Wall Street Journal*, August 20, 2025, sec. Business. https://www.wsj.com/tech/cybersecurity/ai-fake-scam-websites-8a9e0ef6.

SPF Insider. 2025. "Operation FRONTIER+: A Unified Front Against Transnational Scams." Police.Gov.Sg. August 2025. http://www.police.gov.sg/Media-Hub/Police-Life/2025/08/Operation-FRONTIER-A-United-Front-Against-Transnational-Scams.

Subra, Muthesh. 2025. "Cybersecurity Still Not a Priority for Businesses, Say Experts." Free Malaysia Today | FMT. October 12, 2025. https://www.freemalaysiatoday.com/category/nation/2025/10/12/cybersecurity-still-not-a-priority-for-businesses-say-experts.

Surachanee Sriyai. 2025. "Borderland Scam Centres and Cyber Threats: Policy Considerations for Thailand" 2025 (No. 60). https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2025-60-borderland-scam-centres-and-cyber-threats-policy-considerations-for-thailand-by-surachanee-hammerli-sriyai/.

Tech For Good Institute. 2025. "Building Resilience Against Digitally-Enabled Scams and Fraud in Southeast Asia: A Whole-of-Society Approach." https://techforgoodinstitute.org/research/tfgi-reports/building-resilience-against-digitally-enabled-scams-and-fraud-in-southeast-asia-a-whole-of-society-approach/.

The Star. 2025. "Deepfake Scam Uses King and PM's Faces to Promote Non-Existent Investment Schemes." YouTube. October 11, 2025. https://youtu.be/be7qa6f2LmQ?si=S1LlpeODJnRKHe0h.

———. 2026. "Google to Require Verification for Financial Ads in Malaysia from April 14, 2026." March 11, 2026. https://www.thestar.com.my/business/business-news/2026/03/11/google-to-require-verification-for-financial-ads-in-malaysia-from-april-14-2026.

The Straits Times. 2025. "No Decline in Online Scam Cases in Malaysia despite Campaigns, Says Minister," August 20, 2025. https://www.straitstimes.com/asia/se-asia/no-decline-in-online-scam-cases-in-malaysia-despite-campaigns-says-minister.

The Vibes. 2026. "RM2.4b Frozen in January as Scam Hotline Proves Critical within 24-Hour 'Golden Period.'" February 27, 2026. https://www.thevibes.com/articles/news/120037/rm2.4-billion-frozen-in-january-as-scam-hotline-proves-critical-within-24-hour-golden-period.

U Mobile. 2025. "U Mobile, Malaysia's First Telco to Deliver Network-Level Scam Protection, Successfully Blocks Over 265 Million Attempts with Cellusys." December 2025. https://www.u.com.my/en/about-us/newsroom/press-releases/u-mobile--malaysia-s-first-telco-to-deliver-network-level-scam-p.

Wang, Anyu. 2025. *Data Security and Privacy Protection: A Comprehensive Guide*. World Scientific. https://www.worldscientific.com/doi/abs/10.1142/9789819800285_0001.

We Are Social. 2026. "Digital 2026: Malaysia." https://datareportal.com/reports/digital-2025-malaysia.

Whoscall MY. 2025. "MALAYSIA NEGARA NO.1 DALAM KEBOCORAN DATA PERIBADI, PANGGILAN PENIPUAN MELONJAK 82.81%!" 2025. https://whoscall.com/ms/blog/articles/1541-https---app-adjust-com-1mhsdx9q%EF%BC%9Fadgroup=PressRelease.

Wilson, Micheal, Sarah Williams, and Grace Taylor. 2025. "Blockchain Anonymity and the Challenges of Detecting Illicit Financial Flows," August.

World Bank Group. 2023. "Focus Note: Fraud Risks in Fast Payments." https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf.

Yew Yee Tee. 2025. "Keynote Speech on The Evolving Scam Landscape: Trends and Techniques at SCxSC - MyFintech Week 2025." Securities Commission Malaysia. July 8, 2025. https://www.sc.com.my/resources/speeches/keynote-speech-on-the-evolving-scam-landscape-trends-and-techniques-at-scxsc-myfintech-week-2025.

Yuen Meikeng. 2025. "INTERACTIVE: Fake or Fact? Only Three in 10 Malaysians Verify Info Online." *The Star*, July 23, 2025, sec. News. https://www.thestar.com.my/news/nation/2025/07/23/interactive-fake-or-fact-only-three-in-10-malaysians-verify-info-online.