Between Law and Technology: A Qualitative Study of Online Scam Challenges and Legal Responses in Malaysia

Noraini Ismail[1*], Siti Asishah Hassan[2], Zeti Zuryani Mohd Zakuan[3], Rahmawati Mohd Yusoff[4]

[1,2,3]Department of Law, Universiti Teknologi Mara (UiTM), Cawangan Perlis, Kampus Arau 02600 Arau Perlis, Malaysia.

[4]Department of Law, Universiti Teknologi MARA (UiTM), Cawangan Johor, Kampus Segamat, 85000 Segamat, Johor, Malaysia.

***Corresponding Author**

DOI: https://dx.doi.org/10.47772/IJRISS.2025.909000326

Received: 02 September 2025; Accepted: 08 September 2025; Published: 10 October 2025

ABSTRACT

Online scams represent one of the most pressing cyber threats in Malaysia, causing significant financial losses and eroding public trust in digital technologies. Despite increasing regulatory efforts, online scams continue to evolve through sophisticated methods that exploit legal loopholes, technological gaps, and human vulnerabilities. This study adopts a qualitative, desktop-based analysis to examine the challenges posed by online scams in Malaysia and evaluate existing legal responses through gathered published data were gathered from scholarly literature, policy documents, official reports, and judicial precedents. Using the matic analysis, the results indicate that four key challenges exist namely financial vulnerability and consumer awareness, rapid technological development, divided legal systems and enforcement restrictions. While Malaysia has enacted key statutes such as the Computer Crimes Act 1997, Communications and Multimedia Act 1998, and Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001, there remain gaps in the domains of digital literacy, cross-border enforcement, and victim protection. The article ends by suggesting a more cohesive cyber law policy, more financial literacy initiatives and multi-stakeholder efforts to help protect Malaysian society against internet scams.

Keywords: Online scam, cyber law, digital fraud, Malaysia, qualitative study, legal responses.

INTRODUCTION

Malaysia has been significantly influenced by the emerging digital technologies leading to a radical shift in the socio-economic environment of the country as it primarily affects the manner in which citizens conduct commerce, communicate, and transact financial activities in the country. Though this digital revolution has created unparalleled growth and connectivity opportunities, it has also created new frontiers in malicious practices, especially online scams. These types of fraudulent schemes have already become a widespread and rising cyber menace, causing many people and companies significant financial damages, and increasingly undermining trust in the reliability and safety of digital platforms and technologies. The pervasive nature of online scams is underscored by alarming statistics from various authoritative sources. For instance, reports from Bank Negara Malaysia (BNM) and the Royal Malaysia Police (PDRM) consistently highlight a distressing upward trend in scam-related cases, with billions of Malaysian Ringgit being siphoned off annually. Recent data indicates that between 2021 and April 2024, Malaysians collectively lost over RM3.18 billion to online scams, affecting more than 95,800 victims (Scoop.my, 2025). More acutely, the first half of 2025 alone saw financial losses from online scams reaching RM1.12 billion (BusinessToday.com.my, 2025; The Star, 2025), signaling a persistent and growing menace.

Despite concerted efforts by governmental and non-governmental organizations to combat this scourge, online scams continue to proliferate and evolve. Various preventive campaigns, such as the Sapu Bersih Scammer

initiative and the establishment of the National Scam Response Centre (NSRC) in 2022, have been implemented to raise public awareness and provide avenues for reporting and seeking assistance. However, the effectiveness of these measures is continually challenged by the rapid adaptability and sophistication of cybercriminals. The core challenge lies at the intricate intersection of law and technology: while scammers adeptly exploit emerging technologies such as advanced social media manipulation, sophisticated e-wallets, and increasingly potent phishing software Malaysia's existing legal and regulatory frameworks often struggle to keep pace with these dynamic threats. This inherent lag creates a fertile ground for scammers to operate, exploiting legal loopholes and technological gaps.

This study, therefore, aims to provide a comprehensive qualitative analysis of the multifaceted challenges posed by online scams in Malaysia while critically evaluating the adequacy and effectiveness of the existing legal and regulatory responses. In pursuing this aim, the research is guided by three key objectives: first, to identify and analyze the primary challenges arising from the proliferation and evolution of online scams within the Malaysian context; second, to assess the adequacy and effectiveness of the nation's current legal and regulatory frameworks in addressing the complexities and dynamic nature of online scamming; and third, to propose actionable recommendations for the development of a more robust, integrated, and technology-aligned legal framework, together with complementary strategies, to strengthen Malaysia's overall resilience against online scams.

METHODOLOGY

This research employs a qualitative desktop-based analysis to investigate the challenges of online scams and the efficacy of legal responses in Malaysia. This methodological approach was chosen due to its suitability for exploring complex social phenomena through the synthesis of existing data, without the need for direct data collection from human subjects. The paper uses only secondary sources, including the scholarly publication, governmental reports of major agencies like Bank Negara Malaysia (BNM), the Royal Malaysia Police (PDRM), the Malaysian Communications and Multimedia Commission (MCMC), and the National Cyber Security Agency (NACSA), and judicial cases, and publications by non-governmental organizations (NGOs) that deal with cybersecurity and consumer protection.

The data collected were analyzed systematically using a thematic analysis approach as described by Braun and Clarke (2006). This was to be done via the familiarisation process which involved a detailed reading of all the documents collected to get the complete picture of the discourse of online scams in Malaysia, types of online scams, impacts and legal and institutional response. The second stage was interested in the codification concerns and the juridical response to the codification of the information in systematic way and this determined usual patterns, concepts and ideas on the basis of the question of the research. Some codes were developed with the aim of defining different classes of challenges, such as technological, legal, and social, and certain classes of legal response, such as legislative acts, enforcement measures, and policy initiatives. The third stage was coding, where common themes of the coded information were identified and general conclusions of financial vulnerability, technological development, legal fragmentation and enforcement constraints were established. Lastly, findings and policy implications were summarized into the themes and generated a relatively coherent narrative on which the study findings and discussion were based. This was one step to the meaning of the themes, based on the questions of the research and to come up with action policy implications that would improve Malaysia response to online scamming on legal and institutional level.

A descriptive, thematic, desktop study, together with a rigorous thematic analysis, allows a systematic and comprehensive investigation of how Malaysia is adapting to the dynamic and multi-faceted issue of online scams within the existing legal and technological landscapes. It provides a sound foundation to evaluate the adequacy of current responses and future evidence-based policy and legal change recommendations.

LITERATURE REVIEW

Online frauds represent complex types of fraudulent activities implemented over the Internet, and these are aimed at deceiving people or organizations to obtain illegal financial resources. These scams include a whole

host of methodologies such as phishing, or online scam artists trying to obtain sensitive information by posing as authoritative individuals; e-commerce fraud, or fraudulent tactics in online purchases and sales; highly complex investment frauds promising imaginary returns; emotionally charged romance scams; and fake job offers made with the goal of soliciting personal information or money. A common denominator with all these forms is the abuse of both the digital connection and in many cases, people to commit economic damage.

Global and Regional Context

Online scams, to governments and international bodies, including Interpol, have been taking up to now (and increasingly so) at least the officially recognized international cybercrime, and they generate already in billions of dollars monthly due to their scams (Interpol, 2023). This influx is not limited to any single country but continues to be conducted by syndicates that are often transnational and take advantage of the complexities of cross-border jurisdiction in addition to the anonymity of technology to continue their acts with relative impunity. Southeast Asia, especially has become an epicenter in such activities, and even at some point, a center of its operation (with Malaysia being its most likely target as well as operations location at times). It is a twin reply role that did suggest highly cooperative manner and it would be collaborative steps actually taken on what to counter a clumping of the fraudsters with other stakeholders such as the ASEAN and the Interpol and receive joint cybersecurity.

Legal Framework in Malaysia

The Malaysian response to the increasing threat of internet scam lies in the context of legislation whose intent is, despite being fairly broad-based, disseminated within a multiplicity of key legislative acts that provide a multi-dimensional response to online security and online fraud. Computer Crimes Act 1997 (CCA) is one of the main instrumental tools in prosecuting cybercriminals who are involved in hacking computers or manipulation of data that characterizes many fraudulent activities and therefore is a major foundation of law enforcement against cybercriminals. In line with this, the Communications and Multimedia Act 1998 (CMA) governs the actions of service providers in the communications and multimedia sector and gives an antidote to the transmission of offensive material, the abuse of network facilities, and spamming, which are some of the tricks that are commonly used in scam schemes. Though the Penal Code has historically been biased towards the traditional crimes, it is the identical one that can be used to the online scams since the crimes, namely cheating, criminal violation of trust, and misrepresentation can be regarded as the symptom of the attempt to adjust to the new threats (hacking, identity theft, and online fraud), and in 2024, the Penal Code was amended to punish the cyberscams (hacking, identity theft, and online fraud) even more harshly (BAC, 2025). Anti-Money laundering, anti-terrorism financing and proceeds of illegal activities Act 2001 (AMLA) has also played a key role in dismantling the financial facilities of scams by empowering government agencies to trace, freeze and seize illegal proceeds. Lastly, the Financial Services Act 2013 (FSA) enhances consumer protection in the banking and e-wallet industries by requiring a financial institution to implement fraud-prevention controls and providing redress to victims of scam-related financial losses. Together, these laws create an overlapping system that is aimed at combating the dynamic and intricate world of online fraud in Malaysia.

Despite the existence of such legislative tools, challenges about an effective application of such legislative tools still persist on the areas surrounding jurisdictional issues in cross-border proceedings and provision of appropriate redress to victims. The Malaysian government also acknowledges that it will require reforms, discussion, and enactment of new legislation such as the Cyber Security Act 2024 to continue improving cyber defenses and cyber resilience to new threats (NACSA, 2024; Mayer Brown, 2024). There is also the proposal to amend the legislation on the crimes of cyberspace, and the National Cyber Security Agency (NACSA) is leading the pack in coming up with one bill to address cybercrime to help stem out the current menace (Sonny Zulhuda, 2025).

Theoretical Lens

This study is based on two powerful theoretical frameworks which provide a valuable critical examination of forces in the online scam industry and legal counter-measures. The first one is the Routine Activity Theory,

which has its roots in criminology and assumes that when three conditions are met - a motivated offender, an appropriate target, and the lack of an able guardianship - the crime happens. When applied to scams online, this framework clarifies why the increasing online presence of people provides a pool of appropriate targets, and the anonymity and cross-border characteristics of digital platforms reduce effective protection, which provide opportunities to highly motivated offenders to take advantage of. It mentions the value of digital literacy and effective cybersecurity as the newest types of fraud prevention. The second is the conceptualization of Regulatory Theory which views the adaptability of legal and regulatory systems to rapid social and technological change. Within the framework of online scams, it will assess the capacity of the Malaysian legal framework to react to the changing types of online fraud, the challenges of enforcing the law in cross-border settings, and the continued challenge of striking a balance between technological innovation and social security. The theory emphasises that active, flexible and adaptive regulatory frames are required as cybercrime is dynamic and changing.

FINDINGS AND DISCUSSION

This qualitative desktop work-based study, based on a wide variety of academic sources, government reports, official documents, and court case verdicts in Malaysia in 2010-2025, presents 4 major issues of online scams in Malaysia. All these issues highlight the complexity of the dynamics between technology, human psychology, and a developing juridical framework.

Financial Vulnerability and Awareness Gaps

Among the leading causes of the success of online scams in Malaysia, the overall financial vulnerability and the lack of understanding and critical awareness prevalent among the population deserve being mentioned. Numerous victims regardless of their socio-economic status become victims of the latter scheme because of the low financial literacy level combined with the mentioned ineffective cyber hygiene behavior. These vulnerabilities are effectively capitalised upon by scammers, and in many instances they use social engineering tricks to influence people into sharing sensitive data or handing over money. Of particular concern is the situation when it comes to certain groups of people; old people and rural residents are unjustly selected as the most vulnerable group that is not only digital illiterate but also incompetent in thinking critically to see through the circus of high-technology (EPF, 2024; Sinar Daily, 2025). It is further noted that the majority of the scenarios of the Malaysian scams on the Internet could be of the character of legal dealings and the victims could be fooled in sending money to them and thus, a very critical issue of consumer awareness and education is of paramount importance (BNM, 2025). Numerous awareness efforts by banks and government agencies have not been able to alleviate the fears of being scammed by a significant portion of Malaysians, and the most common worry is that they can be tricked into sending money to criminals (FICO, 2024). This implies that the attempts are underway, but they might not be reaching every section of the population and/or are not effective enough to address the changing strategy of scammers.

Rapid Technological Evolution

The unremitting nature of technological development has posed a daunting challenge to the regulators and law enforcers in the war against online scams. Fraudsters are very dynamic and can use advanced technologies to their benefit, and they can change their tactics much quicker than regulatory systems can adapt. The emergence of sophisticated tools such as deepfakes, which can convincingly mimic individuals' voices and appearances, has added a new layer of complexity to online deception, making it increasingly difficult for victims to verify the authenticity of interactions (Alvarez & Marsal, 2025; Chainalysis, 2025). The widespread adoption of cryptocurrencies and crypto wallets, while offering legitimate financial innovation, has also provided scammers with new avenues for illicit financial transactions, often enabling them to move funds across borders with greater anonymity and speed (Remitano, n.d.). Instant messaging applications, initially designed for seamless communication, are now frequently exploited for phishing, impersonation scams, and the rapid dissemination of fraudulent schemes. This constant technological arms race creates a persistent enforcement lag, where law enforcement agencies struggle to acquire the necessary technical expertise, tools, and legal mandates to effectively investigate and prosecute technologically advanced cybercrimes (Telenor Asia, 2024; SC, 2025).

The Evolving Threat Landscape: Cryptocurrency Fraud and Deepfake Scams

The contemporary digital landscape is characterized by the perpetual evolution of online threats, with cryptocurrency-based fraud and deep fake scams representing particularly salient and formidable challenges. These emerging types of fraud pose significant problems to regulatory bodies, law enforcement agencies and ordinary citizens. The unique aspects of cryptocurrencies, their decentralised structure and their pseudonymous character have predisposed them to fraudulent activities. Such activities include multiple illegal endeavours, such as fraudulent investment operations, phishing, and the utilisation of cryptocurrencies in money laundering operations. Among the most common of such scams is the infamous pig butchering scam, which is an advanced form of fraud. Scammers use the relationship with their victims to seduce them over a period of time to invest in fraudulent cryptocurrency trading platforms. Meanwhile, it has been taken advantage of by bad actors to steal money right out of digital wallets and exchange accounts directly by using corrupted software or malicious phishing links. The anonymity and transnational nature of these transactions present a daunting task to the efforts made by the authorities to trace and prosecute the makers of these transactions, which poses a higher risk to the typical user. At the same time, the new technology of deepfakes, appearing as a potent tool of cheating, has become an efficient weapon. The technology has its foundation in artificial intelligence to create very life-like and fake audio, video, or still images, which may be used to impersonate a trusted person, like a family member, workmate, or even a celebrity. Deepfake voice scams have also been rising, with victims being defrauded out of money when they receive phone calls that sound intense enough to masquerade as the voices of their loved ones or friends. The statistical data show that in recent years, the number of global attempts of deep fake fraud has increased drastically. For example, Malaysian law enforcement agencies are pursuing hundreds of voice-impersonation cases, which have a cost ranging into the millions of ringgit. Such instances of deception highlight the growing challenge of distinguishing the true and the counterfeit in the world of the Internet, and the need to make people more conscious of these issues, employ various security systems, and invent new technologies and ways to detect such fakes.

Fragmented Legal Framework

Malaysia's legal response to online scams, while encompassing several statutes, suffers from a degree of fragmentation. The laws are scattered across multiple acts, including the Computer Crimes Act 1997, Communications and Multimedia Act 1998, Penal Code, Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001, and Financial Services Act 2013. While each of these acts addresses specific aspects of cybercrime or financial misconduct, their disparate nature can lead to overlapping provisions, jurisdictional ambiguities, and complexities in prosecution. This fragmentation often creates a challenging environment for victims, who may struggle to identify the most appropriate legal avenue for redress or to navigate the intricate legal processes involved in reporting and seeking remedies for online scams (Lexology, 2025). Furthermore, the lack of a single, consolidated piece of legislation specifically targeting online scams, unlike some other jurisdictions (e.g., Singapore's Online Criminal Harms Act 2023), can hinder a holistic and proactive approach to combating these crimes. While recent legislative efforts, such as the Cyber Security Act 2024 and amendments to the Penal Code, aim to strengthen the legal framework, the inherent fragmentation can still pose challenges in ensuring a seamless and efficient legal response to the rapidly evolving landscape of online fraud (Mayer Brown, 2024; NACSA, n.d.).

Enforcement and Jurisdictional Challenges

The effective enforcement of laws against online scams in Malaysia is significantly hampered by both domestic limitations and complex cross-border jurisdictional issues. The transnational nature of many online scam operations means that perpetrators often operate from outside Malaysia's borders, complicating investigation, apprehension, and prosecution efforts. The absence of effective international cooperation systems and extradition agreements may pose a big challenge to law enforcement agencies trying to prosecute foreign scammers. In the country, there may be specific cybercrime squads, however, due to limited resources such as lack of trained officers, state-of-art forensic equipment, and proper funding, their performance may be wanting. Additionally, absence of special cybercrime departments by state or local departments can create

disparity in response and slow response once the threat has been detected. The number of scam cases reported alone exerts tremendous pressure on the available enforcement mechanisms which results not only in a backlog but also in lengthy investigations. This has been used to offset the loss, such as RM1.5 billion in recovered losses in over 31,000 scam cases (NST, 2025) but the magnitude of the problem is waiting to be hit. These imposition restrictions, along with the jurisdictional issues, make it a hard pill to swallow to effectively address the problem of online scams, and in most cases, the victims have little to no option, which further promotes a sense of impunity in the offenders.

Strengths of Current Legal Framework

Malaysia has a relatively well-developed regime concerning cyber law when compared to several other ASEAN members. This is established by the enabling law like the Computer Crimes Act 1997, the Communications and Multimedia Act 1998, and the Anti-Money laundering, anti-terrorism and proceeds of illegal acts act, 2001, which have provided most of the regulation in prosecuting different types of cybercrime and finance frauds. Specific agencies have also been established in the country like Malaysian Communications and Multimedia Commission (MCMC), Cyber Security Malaysia that centralize roles relating to infotainment of digital information, inculcation of cybersecurity awareness and providing technical expertise in investigating hacking crimes. These agencies, along with the Royal Malaysian Police (PDRM) and Bank Negara Malaysia (BNM) are all multi-agencies in an ecosystem geared towards online threats. More recent, and possibly involving a higher cost investment in co-operation at the institution level and a more coherent response, is a recent project which involves the creation of a new National Scam Response Centre (NSRC) in 2022. The NSRC works as a central point of attack, where scam victims can report scams, allowing faster exchange of information across the relevant agencies to aid in changing the course of action in ongoing scams. Moreover, the identification of proactive intent in legislation can be interpreted not only in the new legislation but a small adjustment (say, the reform of the Penal code in the year 2024, as well as the Cyber Security Act 2024) can be viewed as the efforts of the regulators in shifting the lawmaking priorities towards cybercrime, since the current developments of the cyber threat have shifted dramatically (BAC, 2025; NACSA, n.d.). All of these cyberspace initiatives show that there is an increasing acknowledgment by the Malaysian government that online fraud is a serious issue, and that a safe environment is its legal and institutional penetrations.

Weaknesses and Gaps

Along with these strengths, there are still some significant weaknesses and gaps that threaten the efficiency of the current Malaysian approach to fighting online scams. A significant issue is that legislation is usually reactive since a law is often adopted or modified only after a new threat has been identified, not by predicting it. Such reactive action results in an ongoing delay between the fast development of scam techniques and the legislative ability to combat it, which gives scammers a chance to find loopholes in the legislation, as laws attempt to navigate through the changes in technology. The other weakness is the lack of specific laws that are focused on online scams. However, Malaysia appears to depend, unlike jurisdictions like Singapore which have enacted the Online Criminal Harms Act 2023, on a series of prior statutes, some of which do provide full coverage, but largely lead to inconsistencies in application, jurisdictional conflict, and confusion on the part of both the enforcers and the victims. Another way that laws coordination can help is by facilitating the prosecution process, offer better protection to victims, and be more thorough to counter digital frauds. Also, the issue of law enforcement is also a very serious issue since there are ways, and the issue of extradition. Cybercrime departments in many countries also do not have enough trained staff, top-level forensics equipment, and enough funds to deal with criminal organizations that are continuously becoming more complex. Most scams also have an international nature, which complicates enforcement since extraditing offenders out of Malaysia to other nations would require an intricate international process that is usually either long or ineffective due to the differences in legal system and diplomatic concerns. Finally, victim compensation systems are not developed properly and most victims become bankrupt. As governments strive to reclaim stolen amounts, this is a long process which often does not lead to full restitution. The absence of an effective and available victim compensation mechanism not only compounds the financial losses incurred

by victims but also erodes the confidence of the society in the ability of the justice system to defend citizens against cyber-based financial fraud.

Towards an Integrated Approach

The endemic issues related to online scams in Malaysia cannot be combated only through legislation but through more coordinated, proactive, and multi-layered intervention that encompasses not only legislative changes but also social education, cross-border cooperation, and the improvement of victim protection procedures. A reform that would help to stop such cybercrime would be codifying existing legislation concerning cybercrime to create a single piece of legislation, an Online Scam Act, or broader Cybercrime Act. This would streamline provisions already contained in multiple statutes, provide a more problem-specific and consistent legal framework, remove confusion and enable online fraud to be prosecuted in a more efficient manner. Interestingly, such activity may also incorporate active efforts in support of the emerging technologies and in anticipation of the future methods of the fraud. The second potential answer to the amount of victims of the scam is to improve the digital literacy campaigns as the insecurity caused by the lack of finances and the general level of ignorance is one of the most fundamental causes. Much-needed awareness on cyber hygiene should be taught to the entire society, including vulnerable population groups such as the elderly and rural population. Digital literacy as a curriculum and policy part of national consciousness would help to create a less digitally vulnerable citizenry, one with awareness and suspiciousness toward scams. In addition, as online scams are inherently transnational, Malaysia needs to reinforce the efforts to collaborate with other nations through the establishment of bilateral and multilateral agreements in order to share information on the issue, conduct joint investigations, and speed up the extradition procedures. Malaysia should also strengthen its enforcement power against transnational criminal groups by participating actively in local and international conferences related to cybercrime. Finally, it needs a more victim-focused resolution in the shape of restorative justice provisions, including the establishment of a special compensation fund supported by financial institutions and confiscated illegal funds. Such a fund would offer the victims immediate relief funding, and other non-financial initiatives, including psychological aid and counselling services, will be supplementary to deal with the emotional and psychological health outcomes of internet fraud. This would all result in a more holistic, stronger system to defend Malaysians against the growing threat of internet fraud.

The Imperative of Multi-Stakeholder Collaboration

Online fraud is multi-faceted and dynamic, and can only be tackled effectively through the concerted and coordinated effort of the diversity of stakeholders. The success of technology companies, financial organisations, non-governmental organisations (NGOs), regulatory agencies and government will be the determinant of a robust cyber ecosystem. Technology companies are co-creators of the digital world and thus have a fundamental responsibility to develop secure systems, install strong user authentication tools, and proactively filter out and remove fraudulent content. This will particularly improve their impersonation and false advertisement policies on social media and e-commerce platforms. As the first line in combating financial fraud, financial institutions play a pivotal role in monitoring suspect transactions, enhancing their ability to identify fraud and customer education on existing scam tactics as mandated by the Financial Services Act 2013 of Malaysia. Non-governmental organisations ensure that these actions are reinforced by ensuring that people are aware of the problem, that victims of fraud are supported, and that even tougher action is enforced against consumers. These organisations may also play a central role in mediating between individuals and formal institutions, and as a source of inquiry and information concerning the emerging scam patterns. Regulatory and governmental agencies, in their turn, have a duty to create and enforce strong legal frameworks, integrate national cybersecurity response reporting, and also actively engage in transnational cooperation to fight the transnational nature of scam networks. The fact that the Malaysian government has initiated the reform of the legal framework in recent years, and the proposed Cyber Security Act 2024, is written about the apparent recognition of these problems. In addition, the country has entered into agreements with other international organisations like Interpol to improve the response capability of both the government and the world. The effectiveness of online scam mitigation largely depends on the harmonious integration and coordinated operation of these various stakeholders that create a holistic, adaptive and integrated approach.

Strategic Recommendations for a Resilient Cyber Ecosystem

In a bid to create a more robust and safer cyberspace in Malaysia and to efficiently counter the changing environment of internet scams, a set of progressive suggestions can be developed, anchored on the above analysis. To begin with, it is essential to enhance the digital literacy and critical thinking skills of the general public. This can be done through enacting vibrant and constantly evolving awareness programs among the populace so that they can be armed with the ability to detect advanced phishing schemes, evaluate the risks involved in the use of cryptocurrencies, and identify the presence of deepfake material. Secondly, the regulatory systems of the country should be highly agile and flexible. This involves the continual revision of current laws and the introduction of new rules to address new risks, and this may be supported by implementing regulatory sandboxing strategies that facilitate innovation, but at the same time safeguard consumer interests. Third, cross-border enforcement systems must be significantly enhanced in consideration of the fact that most of the scams on the internet are transnational. This can be achieved through the harmonisation of laws across jurisdictions, facilitating the easy exchange of intelligence with other jurisdictions, and simplifying extradition procedures in cooperation with other international law enforcement organisations. Fourthly, the creation of multi-stakeholder platforms is also proposed to ensure intelligence sharing in real-time, the introduction of coordinated training programmes and execution of joint response to scam incidents. Fifthly, there should be prioritisation of technological solutions, in particular, focusing on investing in artificial intelligence-driven defence to identify fraud and deepfakes, as well as implementing automated analysis tools to be proactive towards cybercriminals. Lastly, there is a need to enhance the mechanisms of victim support and redress, such as facilitating the reporting process, providing comprehensive legal and psychological assistance, and ensuring the presence of effective financial compensation mechanisms. Such measures will serve both as a tool to mitigate the long-term effects of online fraud on the victims and as a way of restoring the confidence that people have developed in the online ecosystem. The combination of these suggestions can be taken as a definite way in which Malaysia can adjust successfully to a fast-evolving threat landscape and safeguard its citizens against the new forms of cyber fraud.

CONCLUSION

Online scamming in Malaysia is a shrewd and common phenomenon, which seals the problematic gap between the dynamic nature of technology and the restructuring of the legal and regulatory environment. Such qualitative research has established that even though Malaysia has been conducting noble works to ensure that the country has a bare-bones framework of cyber law and other related organs, there are some long-term problems that the government is still struggling with. This can be confirmed by a desktop review of the available literature and official reports. These include significant economic vulnerability, foolishness among citizens, the unstoppable stream of technical growth exploited by fraudsters, degradation of the existing legal system, and the sheer leniency in the enforcement and administration of both law and jurisdiction.

Although the existing legal and regulatory frameworks in Malaysia have made significant progress in addressing traditional trends of cybercrime, the emergence of new threats, including cryptocurrency-related fraud and deepfaking scams, demands an innovative, multilateral, and inventive approach. The effective mitigation of these emerging issues rests on building robust, multi-stakeholder collaborations, proactively adapting regulatory frameworks to keep pace with the rate of technological change, enhancing digital literacy among all strata of society, and further investing in advanced technological solutions. This discussion shows the critical role of being alert at all times, attitude towards innovation and an ethos of collaboration among all concerned stakeholders to effectively shield individuals and businesses against the constant and dynamic threat of online fraud. Through the implementation of such a comprehensive and integrated strategy, Malaysia can aspire to build a safer and more secure digital future for all its citizens.

In the context of mitigation, the findings emphasize that despite the benefits of a multi-layered legal system and efforts to establish specialized organizations, like the National Scam Response Centre (NSRC), a maladaptive nature of the legislation and lack of centralization of efforts remain the barriers to success. Even though the latest Cyber Security Act 2024 is a positive step towards a national infrastructure, it still demonstrates the absence of a thorough and harmonized approach to addressing consumer-level online fraud itself.

The following are some of the actions that this paper recommends to increase the Malaysian response to on line scams by bridging the gap between the law and the technology. The initial step is obviously to develop a specific Online Scam Act that will combine ad hoc solutions and provide a harmony with the legal interpretation. Second, access to digital literacy must be promoted nationwide, in schools and as part of community efforts, particularly reaching vulnerable communities, through school curricula, local projects, and mass media. Third, multi-agency coordination among the BNM, PDRM, MCMC, NACSA, and the NSRC regarding intelligence sharing, joint-investigations, and responding as a single unit should be improved. Fourth, financial sector and telecom companies can contribute to the victim compensatory fund, which includes providing monetary aid at the opportune moment to regain confidence and trust in the country. Finally, Malaysia should expand its level of regional and international cooperation, including the programs of the Asian Economic Cooperation (ASEAN) and Interpol, to enhance the distribution of information, cross-border legal and cross-border diversion actions against scam syndicates across borders.

Such concerted, cohesive measures will assist Malaysia to move toward a programmed and effective defence against online swindles, as well as to ensure that its Canada tool and legislation frameworks are in line with each other in an endeavour to safeguard its population and guarantee the growth of its online economy. The next round of research might be to study the effectiveness of specific digital literacy measures, comparative research with other countries that have adopted consolidated online scam laws and the long-term impacts of the Cyber Security Act 2024 on the cybercrime environment in Malaysia in general.

REFERENCES

1. Alvarez & Marsal. (2025, August 25). *Digital Deception: Fighting Fraud in the Era of Emerging Technology*. Retrieved from https://www.alvarezandmarsal.com/thought-leadership/digital-deception-fighting-fraud-in-the-era-of-emerging-technology
2. BAC. (2025, February 3). *Cybercrime in Malaysia: How the 2024 Penal Code Amendments Protect You*. Retrieved from https:// www.bac.edu.my/bac/cybercrime-in-malaysia-how-the-2024-penal-code-amendments-protect-you/
3. BNM. (2025, March 23). *Feature Article: Building a United Front Against Online Fraud Risk*. Retrieved from https:// bnm.gov.my/ar24b7
4. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101.
5. Business Today.com.my. (2025, August 14). *Online Scams Cost Malaysians RM1.12 Billion In First Half Of 2025*. Retrieved from https://www.businesstoday.com.my/2025/08/14/online-scams-cost-malaysians-rm1-12-billion-in-first-half-of-2025/
6. Chainalysis. (2025, May 28). *AI-Powered Crypto Scams: How AI is Being Used for Fraud*. Retrieved from https:// www.chainalysis.com/ blog/ai-artificial-intelligence-powered-crypto-scams/
7. Cyble. (2024, December 2). *Malaysia;s Fight Against Cybercrime: Two New Bills Tabled*. Retrieved from https://cyble.com/blog/ malaysias-fight-against-cybercrime-two-new-bills-tabled/
8. EPF. (2024, August 9). *3 Popular Online Scams to Avoid in Malaysia*. Retrieved from https://www.kwsp.gov.my/en/w/article/how-to-avoid-online-scam
9. FICO. (2024, May 20). *1 in 3 Malaysians Worried About Being Scammed As Real-Time*. Retrieved from https://investors.fico.com/ news-releases/news-release-details/fico-survey-1-3-malaysians-worried-about-being-scammed-real-time
10. ICLG. com. (2024, November 6). *Cybersecurity Laws and Regulations Malaysia 2025*. Retrieved from https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/malaysia
11. Interpol. (2023). *ASEAN Cybercrime Threat Assessment Report*. Lyon: Interpol.
12. Lexology. (2025, May 27). *Shared Responsibility for Digital Scams*. Retrieved from https://www.lexology.com/library/detail.aspx?g=f4f45f87-9efb-462c-9302-e89a3a38b83e
13. Mayer Brown. (2024, December 19). *Malaysia's New Cyber Security Act 2024. A Summary and Brief Comparative Analysis*. Retrieved from https://www.mayerbrown.com/en/insights/publications/2024/12/malaysias-new-cyber-security-act-2024-a-summary-and-brief-comparative-analysis

14. NACSA. (n.d.). *Cyber Security Act 2024 [Act 854]*. Retrieved from https://www.nacsa.gov.my/act854.php
15. NST. (2025, August 27). *Over 11800 arrested in online scam cases , RM1.5bil recovered says*. Retrieved from https:// www.nst.com.my/news/crime-courts/2025/08/1265987/over-11800-arrested-online-scam-cases-rm15bil-recovered-says.
16. Remitano. (n.d.). *5 Common Crypto Scams in Malaysia*. Retrieved from https://remitano.com/jo/forum/73-how-to-avoid-crypto-scams-5-most-common-crypto-scams-in-malaysia
17. SC. (2025, August 7). *Keynote Speech on The Evolving Scam Landscape: Trends and Techniques at SCx SC My Fintech Week 2025*. Retrieved from https://www.sc.com.my/ resources/speeches/ keynote-speech-on-the -evolving-scam -landscape -trends -and-techniques-at-scxsc-myfintech-week-2025
18. Scoop.my. (2025, January 29). *Online scams in Malaysia cost victims over RM3.18bil in less than three years*. Retrieved from https://www.scoop.my/news/245487/online-scams-in-malaysia-cost-victims-over-rm3-18-billion-in-less-than-three-years/
19. Sinar Daily. (2025, February 27). *Digital Danger: The growing cybercrime crisis among Malaysia's youth*. Retrieved from https:// www.sinardaily.my/article/225616/culture/tech/digital-danger-the-growing-cybercrime-crisis-among-malaysias-youth
20. Sonny Zulhuda. (2025, July 5). *Malaysia's Cybercrime Law Reform Underway.* Retrieved from https://sonnyzulhuda.com/ 2025/07/05/malaysias-cybercrime-law-reform-underway-notes-from-the-cydes-2025/
21. The Star. (2025, August 14). *12bil in losses to online scam in first half of 2025, says Home Ministry*. Retrieved from https:// www.thestar.com.my/news/nation/2025/08/14/rm112bil-in-losses-to-online-scam-in-first-half-of-2025-says-home-ministry
22. Telenor Asia. (2024, October 7). *On A Mission Against Scams in Malaysia.* Retrieved from https://www.telenorasia.com/ stories/ on-a-mission-against-scams-in-malaysia/