PENANG INSTITUTE
ISSUES
2026
04 MAR

ANALYSING PENANG, MALAYSIA AND THE REGION

Caught in the Web: Understanding the Profile of Scam Victims

*By **Dr. Rahida Aini Mohd Ismail** (Project Researcher) and **Muhammad Farhan Yaumil Ramadhan** (Intern)*

Executive Summary

- This study investigates the demographic, behavioural, and psychological factors that make individuals in Malaysia vulnerable to online scams.
- These findings aid policymakers in developing targeted cybersecurity policies and prevention strategies for high-risk groups.
- Raising public awareness of scam victims' profiles also encourages safer online behaviour.
- Commercial banks and institutions can use such insights to strengthen fraud detection and customer protection measures.

Caught in the Web: Understanding the Profile of Scam Victims

*By **Dr. Rahida Aini Mohd Ismail** (Project Researcher) and **Muhammad Farhan Yaumil Ramadhan** (Intern)*

Introduction

The increasing sophistication of cybercriminal tactics continues to pose a formidable challenge to global cybersecurity efforts. One of the most pressing threats today is the surge in online scams. These have evolved rapidly, becoming more complex and difficult to detect. According to INTERPOL, cybercriminals siphoned off more than $1 trillion from victims worldwide in 2023 alone, with investment fraud and human trafficking scams showing particularly alarming growth (World Economic Forum, 2024). This trend is fuelled by the accelerated adoption of new technologies, which, while driving economic progress, also expose critical security vulnerabilities that cybercriminals are quick to exploit.

In Malaysia, the issue has grown increasingly critical, paralleling the rapid expansion of internet access and widespread adoption of digital technologies. The country has made notable progress in strengthening its cybersecurity infrastructure, with the National Cyber Security Agency (NACSA) overseeing national cybersecurity coordination and CyberSecurity Malaysia spearheading various initiatives under the Malaysia Cyber Security Strategy 2020–2024. Despite these efforts, the escalating sophistication of online scams often carried out by cross-border syndicates using AI-powered deception underscores the need for more agile, collaborative, and tech-driven defences. These scams frequently exploit digital platforms to mislead individuals or organisations, aiming to illicitly obtain money or sensitive data. As Malaysia becomes increasingly interconnected, the risks and repercussions of online fraud continue to grow, calling for immediate and effective countermeasures.

Recent developments show a worrying upward trend in cybercrime cases in Malaysia, particularly involving online scams. Over the past three years, the number of reported incidents has surged, with total losses surpassing RM1.5 billion in 2024 alone (Qistina, 2025). Table 1 below presents a summary of online scam cases and associated losses.

Table 1: Online scam cases and losses

Year	Total Reported Online Scams	Total Reported Losses (RM)
2019	13,703	RM539.0 million
2020	17,227	RM511.2 million
2021	20,701	RM560.8 million
2022	25,000	RM850.0 million
2023	34,497	RM1.218 billion
2024	35,368	Exceeding RM1.5 billion

Source: Kuah, Lee, Lim, Li & Vivian. (2024).

Why It is Important to Profile Victims

According to a study by Pitchan et al. (2017), many Malaysians fall victim to online scams due to a lack of understanding and awareness about internet safety. This is often because a significant number of internet users still consider online security trivial and tend to ignore essential safety principles. To effectively address the growing issue of cybercrime, it is crucial to increase public knowledge and awareness on the matter.

Profiling scam victims plays a key role in preventing future fraud; it informs policy development, and enhances public awareness of risk factors. By analysing victim characteristics such as demographics and specific vulnerabilities, authorities can identify recurring patterns and develop targeted prevention strategies. This information also enables better policy-making and resource allocation to support victims and strengthen the criminal justice system. Moreover, public education campaigns based on these profiles can empower individuals to recognise their own susceptibility and take proactive measures to protect themselves from scams. In the next section, we will examine more closely who these scam victims are.

The Profile of Scam Victims in Malaysia

Scams affect people from all walks of life, but certain groups are more vulnerable than others due to specific psychological and social traits. Drawing on insights from a presentation uploaded by the Department of Statistics Malaysia (DOSM) from the *10th Malaysia Statistics Conference 2023*, which highlighted gullibility and susceptibility to persuasion as strong indicators of scam vulnerability, we can begin to understand different victim profiles and how their characteristics make them targets. Based on academic literature and newspaper reports, this article examines the profiles of online scam victims in Malaysia.

(a) Elderly individuals and retirees

"Elderly individuals and retirees" typically refers to those aged 60 and above, some of whom have withdrawn from the workforce, while others may still be working or semi-retired. This group is particularly vulnerable to scams due to several interrelated factors. They may experience reduced

digital literacy, social isolation, and a greater tendency to trust information that appears authoritative or familiar. Combined with limited familiarity with digital technologies, this makes it more difficult for them to verify the legitimacy of online platforms before committing funds. Consequently, they become prime targets for impersonation scams and fraudulent phone calls from individuals posing as officials, relatives, or service providers.

For instance, in September 2025, *The Vibes* reported a case involving a 73-year-old victim who was deceived into transferring RM563,560 to a fraudulent investment scheme promoted on Facebook. The scammers enticed the victim with promises of high returns and even provided fabricated statements showing fake profits of more than RM1.7 million (The Vibes, September 4, 2025).

According to Nurul Faqihah et al. (2024), four key factors increase the elderly's susceptibility to scams: these are age-related cognitive decline, physical limitations, limited digital literacy, and social isolation. Additionally, their higher likelihood of having accumulated savings further attracts scammers, making this group a frequent target of online scams and financial fraud.

(b) Young Adults

Young adults, though tech-savvy, are often overconfident online, making them vulnerable to scams that exploit ambition and curiosity. On 3 August 2025, The Star reported that a 42-year-old clerk lost RM277,580 to an online job scam after clicking a link and communicating via WhatsApp. She was instructed to make upfront payments for supposed tasks and only realised it was a scam when asked to pay again to withdraw her 'returns' (Mysara, 2025).

Supporting this pattern, a study by New and Kong (2023) found that 55.6% of social media fraud victims in Malaysia are aged 21–22. Their heavy reliance on social media and eagerness for quick income or attractive job offers make them especially susceptible to job scams. The study underscores the urgent need for education, awareness campaigns, and policy reforms, while calling for national-level research to better address the growing threat of social media fraud among Malaysian youths.

(c) Educated and High-Income Professionals

Educated professionals represent a somewhat unexpected category of scam victims. Despite their relatively higher levels of income and education, they remain susceptible to investment fraud, including schemes involving cryptocurrency and other online financial products. A case reported by *Malay Mail* on 9 April 2025 illustrates this vulnerability. A healthcare worker in Seberang Perai incurred losses exceeding RM1.2 million after responding to an online investment advertisement on Facebook. Attracted by purported returns ranging from 500 to 800 percent, the victim proceeded to transfer funds into seven separate bank accounts associated with the scheme. No returns were received, and the individual subsequently lodged a police report. (*Malay Mail*, April 9).

This incident reflects a broader trend in Malaysia, where various forms of online scams continue to thrive despite ongoing enforcement measures. Among the most frequently reported are the Macau Scam, E-commerce Scam, Cryptocurrency Scam, Ponzi Scheme, and Non-Existent Loan Scam. According to Mohd Akbal Qamas et al.(2024), the persistence of such fraud is largely due to victims'

limited awareness and the increasingly sophisticated tactics employed by scammers. In many cases, victims only recognise the deception after incurring substantial financial losses.

(d) Emotionally Vulnerable Individuals

Romance scammers often prey on individuals who are socially isolated, recently divorced, or widowed. Their search for companionship makes them more likely to trust strangers online, leaving them open to manipulation. For example, a recent report revealed that a 64-year-old retiree in Selangor lost RM1.98 million after being deceived into making 12 payments to 'redeem' a parcel supposedly containing cash (*The Star*, 2025). Research shows that scammers frequently adopt empathetic and sympathetic tones to build trust before gradually exploiting victims through persuasive tactics (Azianura Hani et al., 2019).

(e) Iliterate-Techno Users

Illiterate users are individuals who perform simple functions of the internet and can perform easy tasks through digital media. They rely on digital tools for basic purposes such as online banking, messaging, or shopping, but lack a deeper understanding of cybersecurity practices (Fernando & Jain, 2022). Unlike elderly victims, this group spans across various age ranges, including working adults and rural users with limited access to digital education. Their vulnerability stems from inadequate awareness of online safety measures rather than cognitive decline or emotional isolation.

They are frequently deceived through phishing emails, smishing (fraudulent SMS), fake banking websites, and AI-generated impersonations. In May 2024, The Rakyat Post reported that a Malaysian woman lost RM5,000 after a scammer used artificial intelligence to mimic her boss's voice, convincing her to make a fund transfer (Fong, 2025).

According to Kuah et al. (2024) and Fong & Abu Bakar (2022), such cases reflect a broader cybersecurity literacy gap among Malaysians, including workers in digital sectors who only use basic online skills or are reluctant to adopt advanced digital tools. Limited exposure to online fraud prevention programmes and overreliance on social media platforms or mobile apps without verification mechanisms make this group highly susceptible to modern, technology-driven scams.

(f) Small Business Owners and Freelancers

Small business owners and freelancers often juggle both financial and communication responsibilities, which makes them particularly vulnerable to scams such as fake suppliers, invoice manipulation, and fraudulent payment platforms. With limited time and resources to invest in cybersecurity, they are frequent targets of email scams and bogus client approaches. In a recent case reported by The Star, a 37-year-old freelance interpreter lost RM572,130 in a cryptocurrency investment scam. She was lured by the promise of a 20% return, which ultimately turned out to be fraudulent (Lawrence, 2024).

Table 2: Victim Profiles, Vulnerabilities, Common Scam Types, and Key Sources

Victim Group	Key Vulnerabilities	Common Scam Types	Key Sources
Elderly & Retirees	Digital illiteracy, social isolation, trusting nature, cognitive decline	Macau scams, parcel scams, impersonation fraud	Nurul Faqihah et al. (2024); Nor Aishah (2025)
Young Adults & Students	Overconfidence, ambitious, high social media use	Job scams, social media fraud, fake investments	New, & Kong (2023)
Educated and High-Income Professionals	Overconfidence in financial literacy, risk-taking behaviour, trust in "official-looking" online platforms, exposure to high-return investment offers	Investment scams, cryptocurrency fraud, Ponzi schemes, fake trading platforms	Malay Mail (2025); Mohd Akbal Qamas et al.(2024); Benjamin (2025)
Emotionally Vulnerable	Loneliness, recent divorce/widowhood, desire for connection	Romance scams, emotional manipulation, fake charities	Azianura et al. (2019);Muhammad Adnan et al. (2025)
Illiterate-Techno Users	Basic digital use, low awareness of cybersecurity	Phishing, smishing, impersonation fraud	Kuah et al. (2024), Fong, F., & Abu Bakar, E. (2024).
Small Business Owners	Overworked, low digital infrastructure, invoice management issues	Business email compromise, fake client scams	World Economic Forum (2024); Anis (2025), Bernama (2025), Camoens, A. (2025)

Table 2 highlights that scam vulnerability cuts across diverse demographic and socioeconomic groups, each with distinct risk factors. Elderly victims are often targeted due to digital illiteracy and isolation, while young adults fall prey to scams exploiting ambition and social media engagement. Educated professionals, despite financial literacy, remain susceptible to sophisticated investment and cryptocurrency schemes. Emotional vulnerability, particularly among the recently divorced or widowed, increases exposure to romance scams. Illiterate techno users face phishing risks due to low cybersecurity awareness, whereas small business owners struggle with scams exploiting weak digital infrastructure. Collectively, the data underscores the need for targeted digital literacy and awareness campaigns across all age and occupational groups.

Table 3: The Total Number of Cases for Age Group from Age 15 to 61+ in the Years 2021 to 2023

Year	Age Groups & Total Number of Cases					
	15–20	21–30	31–40	41–50	51–60	≥61
2021	2,108	9,132	6,582	4,440	2,596	1,399
2022	1,620	8,428	6,871	4,513	2,598	1,449
2023	2,066	10,538	8,928	6,274	4,094	2,595

Source: Department of Statistics Malaysia (2024).

Table 3 shows an overall upward trend in online scam cases from 2021 to 2023, driven largely by a sharp increase across all age groups in 2023. The 15–20 and 21–30 age groups were the only cohorts to record a decline in 2022 before rebounding strongly in 2023. In contrast, individuals aged 31–40 to 61-and-above experienced modest or marginal increases in 2022, followed by substantial rises exceeding 1,000 cases in each group in 2023. This pattern suggests a broadening vulnerability to online scams across adult age categories.

Both the 15–20 and 61+ age groups consistently record lower numbers of reported online scam cases. For individuals aged 15–20, this may be attributed to limited financial autonomy and reduced exposure to high-value online transactions. In contrast, those aged 61 and above are likely to have lower levels of digital engagement, a preference for offline transactions, and greater reliance on family members for online activities. In both cases, the lower figures may also reflect underreporting, as scam incidents involving these groups may be resolved informally or go unreported due to varying levels of awareness or reluctance to lodge formal complaints.

In comparison, the 21–30 age group accounted for the highest number of reported cases in 2023 among all age categories. This trend may be attributed to the high level of internet usage among young adults, many of whom are engaged in tertiary education or the early stages of employment, resulting in greater exposure to online platforms frequently targeted by scammers. Supporting this observation, the 2023 Digital Data Report indicated that individuals aged 25–34 constituted 17.6 per cent of Malaysia's total internet users, representing the largest share across all age groups (Kemp, 2023).

A similar pattern is observed among individuals aged 31–40, who also represent a highly active segment of internet users. As a group that is more established in the workforce and regularly engaged in online banking, e-commerce, and digital communication, they remain exposed to online scam risks despite greater professional experience. The DOSM ICT Use and Access by Individuals and Households Survey Report in 2023 further indicates that the age groups with higher levels of Internet usage are also more susceptible to online crime. For individuals aged between 41 and 50, although they remain greatly exposed to scam risks, they record a lower number of reported cases compared to

the younger age groups. Meanwhile, those aged 51–60 show even lower figures, which may be associated with reduced digital engagement as many in this group are approaching or have reached retirement age.

Policy Recommendation: Segment-Specific Awareness Campaigns

The profile of scam victims in Malaysia underscores the urgent need for a multi-pronged national response that goes beyond technical fixes. There is a great requirement for a segment-specific awareness campaign to strengthen public resilience, inform targeted interventions, and support more effective enforcement.

Public education strategies need to reflect the diversity of scam victims across age, income, and digital literacy levels:

- Targeted messaging: Develop campaign content tailored to key groups such as the elderly, youth, professionals, and emotionally vulnerable individuals.
- Platform-appropriate outreach: Use social media (e.g., TikTok, Instagram) to reach youth, while traditional media like radio and television can be more effective for older demographics.
- Simulation-based training: Incorporate real-life scam scripts and interactive elements in campaign materials to help the public recognise common manipulation techniques.

Conclusion

Online scams represent a growing threat to Malaysia's digital economy and social fabric. Losses now exceed RM1.5 billion annually, with victims spanning all social, age, and income groups. Vulnerability is not limited to those with low digital literacy like overconfidence. Emotional distress and lack of awareness are equally critical risk factors.

By profiling victims, we gain insight into not only who is being targeted, but why. This knowledge is vital in designing prevention strategies that are more inclusive, responsive, and effective. As Malaysia deepens its digital transformation journey under national frameworks such as *Malaysia Madani* and *Penang2030*, strengthening public cyber resilience must be prioritised.

The policy path forward lies in sustained collaboration across sectors that include government, law enforcement, civil society, educational institutions, and the private sector. With the right blend of technology, education, and regulation, Malaysia can build a safer digital future for all.

References

Anis, Z. (2025). Paying for nothing: How Malaysians are scammed using parcels they never ordered. *The Malay Mail*, 17 June. https://www.malaymail.com/news/malaysia/2025/06/17/paying-for-nothing-how-malaysians-are-scammed-using-parcels-they-never-ordered/179959

Azianura Hani at al. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *Journal of Language Studies*. Vol. 19(1).

Benjamin, N. (2025). Two teachers, lecturers, lost over RM400,000 to investment scams. *The Star*, Oct 13. https://www.thestar.com.my/news/nation/2025/10/13/two-teachers-lecturer-lose-over-rm400000-to-investment-scams

Bernama. (2025). Penang woman loses over RM2.3m in 'love scam' with alleged Singaporean. https://www.malaymail.com/news/malaysia/2025/08/09/penang-woman-loses-over-rm23m-in-love-scam-with-alleged-singaporean/187018

Camoens, A. (2025). Police: E-commerce scams cost Malaysians RM63mil in six months. *New Straits Times*, https://www.nst.com.my/news/crime-courts/2025/07/1249250/updated-police-e-commerce-scams-cost-malaysians-rm63mil-six-months

Department of Statistics Malaysia. (2023). ICT use and access by individuals and households survey report 2023 (ISSN 2289-7240). Department of Statistics Malaysia. https://storage.dosm.gov.my/icths/icths_2023.pdf

Department of Statistics Malaysia. (2024). Crime statistics Malaysia 2024 (ISSN 2637-0786). Department of Statistics Malaysia. https://storage.dosm.gov.my/crime/crime_2023.pdf

Fernando, J.G & Jain, S.K. (2022). Digital Illiteracy of teachers and its impact in online learning. Technoaret Transactions of Applications of Informations of Communications Technology (ICT) in Education, Vol.1 (3).https://www.researchgate.net/publication/369290769_Digital_Illiteracy_of_Teachers_and_its_Impact_in_Online_Learning

Fong, F. (2025). Woman loses RM5K after answering a call from "Boss". https://www.therakyatpost.com/news/malaysia/2025/05/14/woman-loses-rm5k-after-answering-a-call-from-boss/

Fong, F., & Abu Bakar, E. (2022). The factors causing consumers to fall victim to online shopping scams. *Jurnal Pengguna Malaysia*, Jilid 1, Vol.38, 17-26.

Kemp, S. (2023, February 13). *Digital 2023: Malaysia*. DataReportal. https://datareportal.com/reports/digital-2023-malaysia

Kuah, Y.C., Lee, W.X., Lim, N.H.,Li, L.Y & Vivian. (2024). Awareness on online financial scams: A case study in Malaysia. *International Journal of Advanced Research in Economics and Finance*. Vol. 6 (1). 101-116.

Lawrence, A. (2025, The Star). Freelance interpreter cheated out of over RM570,000 in a crypto Investment scam. https://www.thestar.com.my/news/nation/2025/09/19/freelance-interpreter-cheated-of-over-rm570000-in-crypto-investment-scam

Malay Mail. (2025, April 9). Healthcare worker loses over RM1.2 million in Facebook investment scam. https://www.malaymail.com/news/malaysia/2025/04/09/rm12m-lost-medical-staff-falls-for-fake-facebook-investment-promise/172378

Malay Mail. (2025, April 9). RM1.2m lost: Medical staff falls for fake Facebook investment promise. https://www.malaymail.com/news/malaysia/2025/04/09/rm12m-lost-medical-staff-falls-for-fake-facebook-investment-promise/172378

Malaysia Cyber Security Strategy, 2020-2024. https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf

Mohd Akbal Qamas et al. (2024). The impact of financial literacy on online financial scam victimization. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, Vol. 14(4).

Muhammad Adnan, P., Ali, S., & Nadhirah, M.A. (2025). A Systematic Literature Review on Online scams: Insights into digital literacy, technological innovations, and victimology. *Jurnal Komunikasi: Malaysian Journal of Communication*, Jilid 41(1), 107-124.

Mysara, F. (2025). Clerk loses over RM277, 580 in an online job scam in Muar. The Star, August 3. https://www.thestar.com.my/news/nation/2025/08/03/clerk-loses-over-rm277580-in-online-job-scam-in-muar

New, K & Kong, ZX. (2023). Exploring teenage awareness of social media fraud in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, Vol. 13(12).

Nurul Faqihah et al. (2024). Scam issues among the elderly: A conceptual paper. International *Journal of Academic Research in Business and Social Sciences*, Vol. 14(10),1624-1634.

Pitchan, M. A., Baco, M. A., Hassan, F., & Ghazali, A. H. A. (2022). Knowledge, attitudes, practices towards information privacy & security of online purchase by youth. *Jurnal Komunikasi: Malaysian Journal of Communication*, 38(4), 250–267. https://journalarticle.ukm.my/21571/1/55775-200453-1-PB.pdf

The Vibes. (2025, September 4). Retiree loses nearly RM600,000 to a non-existent investment scheme. https://www.thevibes.com/articles/news/112341/retiree-loses-nearly-rm600000-to-non-existent-investment-scheme

The Star. (2025, August 31). Retired banker loses RM1.98mil to 'love scam'. https://www.thestar.com.my/news/nation/2024/08/31/retired-banker-loses-rm198mil-to-039love-scam039

The Star. (2025, February 26). 60 Malaysians rescued from job scam syndicate in Cambodia, says Wisma Putra. https://www.thestar.com.my/news/nation/2025/02/26/60-malaysians-rescued-from-job-scam-syndicate-in-cambodia-says-wisma-putra

The Vibes. (2025, September 16). University lecturer and woman lose over RM5 million in separate investment scams. The Vibes. https://www.thevibes.com/articles/news/112818/university-lecturer-and-woman-lose-over-rm5-million-in-separate-investment-scams

Qistina, S. (2025). Cybercrime losses exceed RM1.5bil in 2024. New Straits Times, February 18. https://www.nst.com.my/news/nation/2025/02/1176474/cybercrime-losses-exceed-rm15bil-2024

World Economic Forum. (2024). 'Pig-butchering' scams on the rise as technology amplifies financial fraud, INTERPOL warns. World Economic Forum. https://www.weforum.org/stories/2024/04/interpol-financial-fraud-scams-cybercrime/

Managing Editor:
Ooi Kee Beng

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

PENANG INSTITUTE
making ideas work

10 Brown Road
10350 George Town
Penang, Malaysia

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