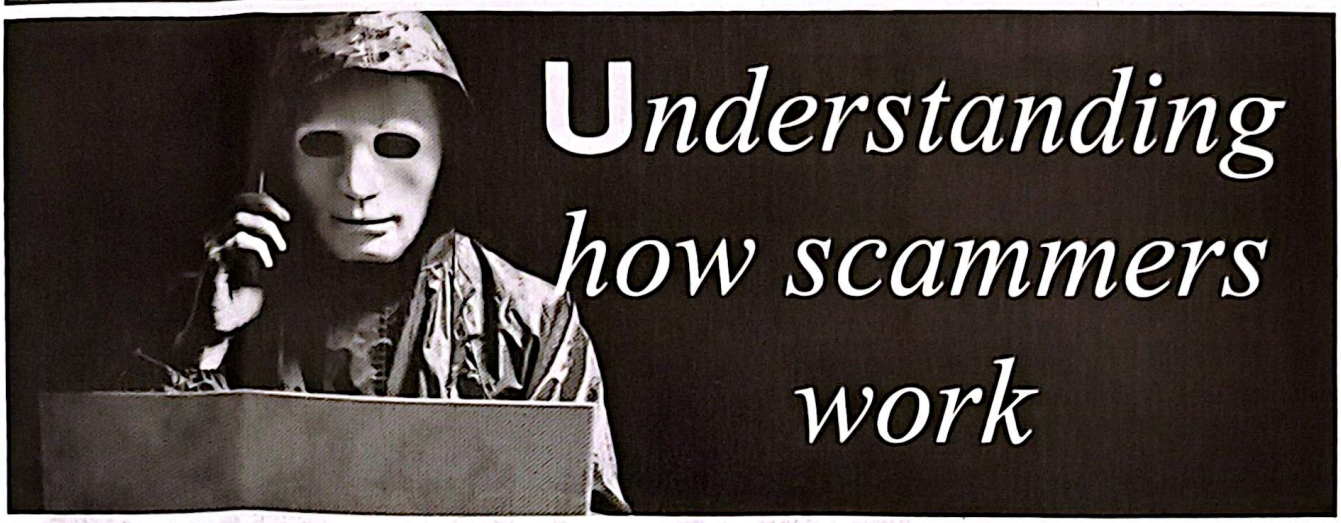
THURSDAY
cybertech

A look at the latest innovations and issues in the world of cyber technology and how they impact our lives.



Understanding how scammers work

Dr Paul Selva Raj

THE number of scams and the associated financial losses have been significantly increasing over time. In 2023 alone, reported scams resulted in financial losses totalling RM1.34 billion. This figure, reported by the National Scam Response Centre (NSRC), does not include losses from unreported scams.

Furthermore, senior citizens have been especially targeted. Bukit Aman reported that senior citizens accounted for 20pc of the RM2.7 billion lost to scams between 2021 and 2023 *(pic)*.

According to the NSRC, the top three scams in Malaysia include e-commerce, loan and investment fraud. Between January 2021 and August 2023, 26,663 e-commerce, 10,759 loan and 9,640 investment scams were reported.

As for investment scams, the financial losses more than doubled from RM209 million in 2022 to RM437 million in 2023. While the financial losses are often the main focus, the psychological impact on individuals as well as the resulting social problems should not be ignored.

Victims frequently experience depression and anxiety, and scams can also negatively affect family and social relationships.

Consumers are increasingly going online to make payments and are extensively using new social media platforms such as Facebook, Instagram, and Twitter. Consequently, the online medium and social media have become breeding grounds for scammers to reach vulnerable consumers.

In most cases, scam victims are unable to recover their losses. While authorities can take action to compel banks to be more cautious and to implement stricter security measures to minimise risks to consumers, individuals must also play a critical role in protecting themselves.

When it comes to scams, the best protection is self-protection.

Scams are continually evolving, taking on various and sometimes innovative forms. Consumers should always stay updated about the latest scams and scammers' tactics. For example, it has been recently reported that scammers are implanting malware in digital wedding invitation cards. Even wedding invitations may not be safe.

Scams rely on multiple strategies to ensnare their victims, with the most common being emotional manipulation.

Scammers often use fear-based tactics such as impersonating police officers, anti-corruption officers, customs officials or income tax authorities.

Scammers often create situations involving urgency and tight deadlines, such as the threat of arrest or promises of high returns if invested immediately.

These tactics are designed to pressure individuals into making hasty decisions they would not typically make. This "attack" prompts an emotional reaction rather than a deliberate and considered response.

Another common tactic, especially in investment scams, is the sunk cost strategy.

Scammers trick people into investing small amounts initially, making them feel compelled to invest more because they have already spent some money, hoping to eventually recover their investment.

Scammers may also exploit the latest government assistance programmes by targeting potential beneficiaries for scams, such as cash aid initiatives.

They adapt their messages to align with the specifics of the latest government schemes to deceive people.

Apart from the major scams mentioned, such as Macau scams, job scams and love scams, there are numerous other types of scams.

Each scam often necessitates a unique strategy for self-protection. Here are some general tips:

Pause and verify: When contacted via call, email or messaging apps requesting personal or banking information, especially under urgent or threatening claims (like from the police, income tax department or your bank) – pause a moment. Do not respond immediately. Scammers create urgency to provoke quick responses. Stop and consult with someone you trust, and carefully consider your actions.

Never transfer money: Banks never ask clients to transfer funds over the phone or via email. Be cautious if someone requests your account details to pay for services or jobs.

Verify source: Always verify the legitimacy of requests for personal details or money transfers. Use trusted sources for contact information. Avoid calling numbers provided by the scammer. Verify official contact details from the organisation's website and contact them directly.

Avoid unrealistic promises: Be wary of promises of high returns with low risks. If an offer sounds too good to be true, it likely is.

Report suspicious activity: If you encounter a scam or suspicious activity, promptly report it to the relevant authorities such as the National Scams Response Centre or the police. Your report could prevent others from becoming victims.

Scams are becoming increasingly sophisticated. It is crucial for consumers to stay informed and continuously educate themselves to protect against these threats.

The Federation of Malaysian Consumers Associations (Fomca) urges authorities to intensify efforts in empowering consumers, especially vulnerable groups, through ongoing anti-scam campaigns.

Regulators must prioritise consumer education to enhance awareness and self-protection. – The Sun

● **The writer is the deputy president of Fomca.**