**MINORITY SHAREHOLDERS WATCH GROUP**

*BADAN PENGAWAS PEMEGANG SAHAM MINORITI BERHAD*

(Incorporated in Malaysia – Registration No.: 200001022382 (524989-M)

New Straits Times, Business Times – Thursday, 23 November 2023

SCAM ACTIVITIES

# THE PSYCHOLOGY BEHIND DECEPTION

DEVANESAN EVANSON

BANK Negara Malaysia and the Securities Commission are constantly and consistently reminding us of the numerous types of scams out there.

They advocate a stance of "buyer beware" and exercise healthy scepticism. They have produced alert lists for us to be wary of some of these fraudsters. They exhort us to do business with licensed entities and people.

Nevertheless, we continue to receive calls and propositions to convince us to part with our money, only for it to end up as someone else's ill-gotten gains. Tracing fraudsters is not easy in the current muti-jurisdictional layered scenario.

We may have received phone calls telling us that some amounts have been charged to our credit cards. Or the calls may be from some government authority like the inland revenue board, the courts, the customs, or the police, telling them that some terrible thing is about to befall us if we do not act quickly. Almost all of these are pre-recorded messages, and a fitting reaction would be to terminate the call — immediately.

Then there are those that sound a bit more convincing because these are not taped calls to sound even more convincing, they are able to quote details about us, like our address or our identification number.

The fitting response would be to hang up and call back the entity involved to clarify.

In an ever-evolving digital landscape, scams continue to adapt and exploit unsuspecting individuals. From phishing emails to investment fraud, scammers employ various tactics to deceive people. Understanding the latest scams and the psychology behind why people fall for them is crucial in building resilience against such threats.

**Phishing attacks:** Phishing remains a prevalent scam, with attackers using deceptive emails, messages or websites to trick people into revealing sensitive information. These messages often appear legitimate, imitating reputable organisations or individuals. People fall for them due to the clever use of social engineering, exploiting trust and urgency to prompt quick actions.

**Crypto scams:** As the popularity of cryptocurrencies rises, so do scams associated with them. Fraudsters may create fake cryptocurrency exchanges or investment opportunities, promising quick and significant returns. The allure of easy wealth, coupled with a lack of understanding of the complex crypto world, makes individuals susceptible to these scams.

**Social media scams:** With billions of users on social media platforms, scammers exploit these networks for various schemes. Fake profiles, romance scams, and fake giveaways are common tactics. The desire for social connection and the promise of exclusive opportunities make people more likely to engage without verifying the legitimacy of the source.

**Tech support scams:** Tech support scams involve fraudsters posing as technical support agents, claiming that the victim's computer has a virus or security issue. The fear of losing data or compromising personal information often drives individuals to comply with the scammer's instructions, leading to financial losses or identity theft.

**Impersonation scams:** Scammers may impersonate government officials, law enforcement, or utility providers, creating a sense of urgency to extort money or sensitive information. The fear of legal consequences or service disruptions prompts victims to act hastily without proper verification.

## Understanding the psychology

**Emotional triggers:** Scammers exploit emotions like fear, greed, and curiosity to manipulate their targets. Phishing emails often create a sense of urgency, prompting individuals to act without careful consideration. Emotional responses can override rational thinking, making it easier for scammers to succeed.

**Lack of awareness:** Many victims fall for scams due to a lack of awareness about the latest tactics. Scammers adapt, using sophisticated techniques that may go unnoticed by individuals who are not updated on current scam trends. Awareness campaigns and education are essential in building resilience against evolving threats.

**Trust in authority:** People tend to trust figures of authority, whether it is a government official, a bank representative, or a tech support agent. Scammers exploit this trust by impersonating such figures, leading individuals to believe the information they receive is legitimate. Verifying the identity of the person or organisation is crucial in avoiding such scams.

**Desire for quick gains:** The promise of quick and substantial gains is a common tactic in investment scams. The desire for financial success can cloud judgment, leading individuals to invest without conducting thorough research. Understanding that genuine opportunities require careful consideration can mitigate this risk.

**Social connection and influence:** Social media scams often leverage the desire for social connection and the influence of peers. Seeing others engage in a seemingly beneficial opportunity creates a sense of "FOMO" (Fear of Missing Out), driving individuals to participate without questioning the legitimacy of the offer.

Combating scams requires a multi-faceted approach that includes awareness and understanding of the psychological factors at play. Individuals must stay informed about the latest scams, develop a healthy scepticism and prioritise verification over immediate action.

Education campaigns, cybersecurity measures and promoting a culture of cautious online behaviour are essential components in the ongoing battle against scams. By addressing the root causes and psychological triggers, society can collectively build a more resilient defence against the ever-evolving landscape of fraudulent activities.

---

The writer is chief executive officer of Minority Shareholders Watch Group.