



Preventing emotional manipulation by online scammers

We cannot ignore the high costs of online scams in society – especially the psychological distress, says the writer.

By ARMAN RASHID

THERE is growing alarm about the prevalence and consequences of online scams affecting Malaysians.

According to the Malaysian Communications and Multimedia Commission's Internet User Survey 2022, 68.5% of respondents experienced online scams and fraud (an increase of over 21% since 2020). Royal Malaysia Police (PDRM) statistics meanwhile showed that there have been 32,462 reports of online scams (up from 25,480 in 2022) amounting to financial losses of about RM1.3bil since January this year.

Unsurprisingly, a recent regional study by Telenor Asia (2023) found that Malaysians are paradoxically one of the best connected, yet most concerned about online safety. After all, online scams have continued unabated despite public awareness campaigns about digital security. In the first five months of 2023 alone, the Malaysian government reported RM330mil was lost to online scams on Meta platforms (Facebook, Instagram and WhatsApp).

These rampant cybercrimes have raised concerns about an epidemic of scams – “scamdemic” – a term coined by the United Nations Office on Drugs and Crime (UNODC).

We cannot ignore the high costs of online scams in society, taking into account both financial losses and emotional distress. This calls for a better understanding on the evolution of online scams, emotional manipulation by scammers, and most importantly emotional safeguards to protect ourselves from falling prey.

Emotional manipulation

In the social media era, online scams are tailor-made, real time and personalised to build rapport with targeted victims from different backgrounds. Notwithstanding

stereotypes of older or less educated people falling victim to online scams, in reality people from all backgrounds may be susceptible to emotional manipulation by scammers. These online scammers have become highly sophisticated technologically and emotionally to exploit our emotions, including trust, desires and fears.

In many cases, online scammers have been able to defraud even tech-savvy internet users by appealing to our innate emotional needs, in particular financial security and emotional attachment. They have been able to do so by nurturing different types of online interactions ranging from friendships to intimacy with the 5As of relationship building – attention, affection, appreciation, acceptance and approval. This typically helps establish a high level of emotional trust with targeted victims before online scammers solicit money, whether it is for purported investment schemes or supposed lovers in crisis.

Such growing emotional dependence on online scammers is designed to hinder our rational thinking processes, often leading to lower self-control and higher risk-taking behaviour. We tend to ignore red flags (for instance, inconsistent knowledge about professed cultures) as a result until it is too late. In some cases, this may be because of our cognitive biases, including optimism bias overestimating positive events, overconfidence bias presuming digital safety skills, truth bias seeking to believe others and confirmation bias searching information reinforcing our beliefs.

Moreover, online scammers often target potential victims undergoing life challenges like divorce, grief and unemployment that may result in financial or social insecurity. Another form of common digital fraud manipulating our emotions is impersonation of government agencies or financial institutions purportedly owing

money from us. This takes advantage of our respect for authority, particularly in high power distance cultures like Malaysia, in demanding immediate access to bank accounts or financial payments.

These days online scams often take the form of sales pitches creating a sense of urgency, solution and fulfilment, while building incremental trust through foot-in-the-door techniques before defrauding large amounts of money. The personalised nature of digital fraud requires better cybersecurity awareness and emotional safeguards against online scammers. How can we reduce our vulnerability to online scams?

Emotional safeguards

There needs to be awareness not only about emotional manipulation by online scammers, but also self-awareness about our own emotional states, life aspirations and cognitive biases and personality traits that make us vulnerable to digital fraud in the first place. In fact, self-awareness is the first step against falling prey to online scams. This process involves self-discovery, emotional awareness, and in some cases help-seeking to exercise restraint irrespective of baits used by online scammers.

> **State of mood:** Recognising mental health stressors make us more vulnerable to online scams, we require have regular check-ins on our emotional state. There is need for consciousness on mood conditions increasing our risks of falling prey to fake offers of security and comfort by online scammers during difficult life situations. If we fail to remain vigilant in stressful period, online scammers may leave us in a worse emotional state.

> **Emotional requirements:** We need to be conscious about our emotional needs and wants that may be exploited by online scammers. This requires emotional

introspection about our innermost feelings and desires, for instance, getting rich quick, feeling loved or fearing of missing out. There is no need for judgement about these emotional requirements, but self-awareness can go a long way in remaining alert against online scams.

> **Cognitive biases:** Many of us overestimate positivity, presume digital safety, believe humans are truthful and prefer information reinforcing our comfort zones. Such tendencies of cognitive biases in our personalities may result in imprudent decisions, including trusting online scammers. Though it is not in our interest to be overly suspicious in every life situation, there is room for cautious decision-making to avoid online scams.

> **Self-control and risk-taking:** The prevalence of online scams can be reduced with better awareness on our levels of self-control and risk-taking behaviour. The propensity for low self-control and high risk-taking behaviour may lead to impulsive decisions, for instance transferring money for love or investments without calculating risks. These personality traits may result in errors of judgement, including ignoring red flags shown by online scammers.

> **Social support:** Social relationships can serve as an important protective factor against online scams. In the post-pandemic period, a healthy balance between social and in-person socialisation may reduce risks of potential emotional dependence on online scammers. Sharing experiences with social networks can help look out for potential red flags at an earlier stage, as well as seek emotional support in the aftermath of online scams.

> **Professional support:** Mental health professionals can support scam survivors regain their sense of security, trust and confidence after traumatic heartbreaks and financial losses. It is important for scam survivors to seek profession-

al help if there are prolonged emotional responses, including anxiety, fear, shame, anger and guilt. There are various forms of mental health services like helplines, chat apps and counselling available for scam survivors to prevent the onset of long-term mental health conditions and develop resilience against online scams.

Emotional resilience

Given the evolving nature of emotional manipulation by online scammers, we have no choice to be one step ahead of the game with emotional resilience. Greater self-awareness of our mental state, emotional requirements and cognitive biases will help reduce our vulnerability to online scams. This will help us leverage the positives of internet and social media to build human connections transcending borders, while remaining vigilant against digital fraud.

Prevention is better than cure – emotional resilience is the best protection against emotional manipulation by online scammers. The “scamdemic” industry will itself be likely to collapse if there are fewer of us who fall prey to their criminal activities. Till then, we must remember to remain alert – if it is too good to be true, it probably is.

Dr Arman I. Rashid is a policy analyst turned mental health counsellor, family dispute resolution practitioner and mediator.

If you suspect you have fallen victim to a scam, call the National Scam Response Centre at 997 within 24 hours.

For those in need of mental health support, reach out to Talian Kasih (15999 or WhatsApp 019 2615 999), Befrienders Kuala Lumpur (03-7627 2929 or befrienders.org/my), or message Thoughtfull, a chat-based online mental health service to improve wellbeing (www.thoughtfull.world/online-mental-health-therapy).

