Opinion

How AI and social media are giving scammers an edge

By Vijay Varadharajan
November 1 2023 - 1:12pm

Online scams are a common way cybercriminals compromise people's online financial accounts, personal health records and other sensitive information. Their goal is to trick victims into paying money or giving away personal information. They use email, text messages, phone calls or social media, often pretending to be a person or organisation the victim trusts.

Social media scams have become more prevalent, with staggering losses recorded. A US Federal Trade Commission report indicates $2.7 billion was lost to social media scammers from January 2021 to June 2023, higher than any other method of contact.

How AI and social media are giving scammers an edge

Social media gives scammers an edge. They can easily manufacture fake personas, or hack into the victim's profile, impersonate the victim, and con the victim's friends. They can tailor their approach from what someone shares on the social media. Scammers can also use advertising tools to methodically target someone based on personal details like age, interests, or past purchases.

UK's Global Anti Scams Alliance says around 10 per cent of UK adults fell prey to a scam in the last year, while 53 per cent came across more scams than usual. In Australia around $200 million was lost to scammers so far this year, with over 100,000 scams reported to the Australian Competition and Consumer Commission.

While online shopping scams often generate the highest number of reports, the largest dollar losses are from social media scams promoting fake investment opportunities. Scammers promote their supposed investment success to lure people to bogus investment websites and apps.

Romance scams are the second highest cause of losses on social media, with many beginning on Facebook, Instagram, or WhatsApp. These often start with a seemingly innocent friend request from a stranger followed by love bombing, and the inevitable request for money.

People can protect themselves and reduce the chance of becoming a victim to social media scammers.

Limit who can see your information on social media. All platforms collect information from your online activities, so set restrictions on your privacy settings. If a friend messages you about an opportunity or urgently needing money, call them. Their account may have been hacked, especially if they ask you to pay by cryptocurrency or wire transfer. If someone appears on your social media and rushes to start a friendship or romance, slow down and check their credentials through alternate channels. Do your research, and never send money to someone you haven't met in person. Before you buy, check out the company - search online for its name plus "scam" or "complaint".

Generally, if you receive an email asking for personal information or offering something that looks too good to be true, don't click links or provide information. Only download from trusted websites and app stores.

Technology including AI is a double-edged sword with cyber security. AI can provide benefits by enabling advanced techniques to detect and prevent malicious attackers. However, AI also helps cybercriminals easily create and personalise scams making them more convincing,

tailoring them to victims using personal information sourced from social media and other online activity.

AI can be used to create deepfake audio and video clips to trick victims. Recently, there has been an alarming trend of AI use to create scams by mimicking voices of loved ones in distress. With a spoofed call showing the loved one's number on caller ID, scammers may claim to be in serious trouble and beg for money. That fake scenario can be convincing, motivating the victim to respond to the request out of genuine concern for a friend or relative.

To protect against voice cloning scams, always be sceptical when asked for money in any form. Don't rely on caller IDs as they can be faked. Hang up and call the person using a number you know to be theirs.

Learn to recognise the ingredients of a scam, like pressure to act immediately, scare tactics or enticing offers, demands for money in unusual forms, and requests for sensitive or personal information.

If an offer looks too good to be true, it probably is.

Professor Vijay Varadharajan is the global innovation chair and chief cyber strategist at the University of Newcastle