

Media Title : The Sun
Headline : AI scams get real
Date : 21 September 2026
Section : LYFE
Page : 22



AI-generated deepfakes can make fake celebrity endorsements and investment promotions appear genuine. – **MAGNIFICPIC**



Scammers are using AI to clone voices and create convincing impersonations of bosses, family members and public figures. – **PIC FROM SINGAPORE POLICE FORCE**

■ BY **MARK MATHEN VICTOR**

A phone call from your boss. A video featuring a celebrity. A message from a family member asking for urgent help. All three could be fake.

Artificial intelligence (AI) is giving scammers new tools to make familiar fraud schemes more convincing, allowing them to clone voices, generate realistic images and videos and produce polished messages in seconds.

The technology is changing the problem from spotting obvious scams to verifying things that look and sound increasingly real.

Malaysia has already seen several cases involving AI-generated impersonation. In one reported case, a woman in Selangor lost RM5,000 after scammers used a voice clone to impersonate her employer and requested Touch 'n Go PINs.

Police have also warned about so-called "silent calls", in which victims receive calls that appear to contain no one on the other end. Authorities have warned that scammers may use these interactions to obtain voice

AI scams get real

► Voice clones, deepfakes giving fraudsters new ways to impersonate people, brands

samples that can later be used for cloning.

The technology has also entered fake investment promotions.

Deepfake videos can make public figures appear to endorse investment schemes, products or fundraising campaigns they have nothing to do with. Malaysian authorities have warned about the spread of fraudulent AI-generated content, including material impersonating prominent Malaysians.

AI advantage: Scale

A fraudster no longer needs to write every message from scratch or spend hours editing a convincing fake. Generative AI can produce

customised text, images and audio quickly, allowing criminals to target more people with fewer resources.

That also means some of the traditional warning signs are becoming less useful, like how poor spelling and awkward grammar once made many phishing messages easy to identify. AI can now produce fluent, professional-sounding messages.

A robotic-sounding voice was another giveaway. That is becoming less reliable too as recent research into synthetic speech found that people struggled to identify some AI-generated voices, particularly when only parts of a genuine recording had been manipulated.

So what should consumers look for?

The biggest warning sign may have little to do with the quality of the fake. Instead, it is the request.

Verify before trusting

An unexpected demand for money, passwords, PINs or verification codes should trigger caution, particularly when the sender creates a sense of urgency. A familiar voice should not automatically be trusted either.

If someone claiming to be a family member asks for an urgent transfer, call them back using a number you already have rather than continuing the conversation through the incoming call.

The same principle applies at work. An apparently genuine request from a manager to make a payment or reveal sensitive information should be verified via

another channel.

And when a celebrity appears in an online investment advertisement, the safest assumption is not that the video proves anything.

Malaysia's growing exposure to AI-generated scams comes as authorities grapple with a broader rise in online fraud. The Digital Ministry said Malaysia recorded 12,110 online scam cases involving fraudulent activities in the first three months of 2025 alone.

As it stands, AI is not replacing the old scam playbook. It has simply made the playbook harder to recognise and for consumers, the most effective response is surprisingly low-tech: Stop, check, call back and verify.

In an age when a voice, a photograph or a video can be manufactured in minutes, seeing and hearing something is no longer enough to prove that it is real.