

Media Title : Asia Times (Pulse)
Headline : Use family password to outsmart scammers: Expert
Date : 27 June 2026
Section : National
Page : 5



Use family password to outsmart scammers: Expert

► 'Employ verification questions, security phrases or words known only to close ones to beat AI voice-cloning technology'

■ BY T.C. KHOR
newsdesk@thesundaily.com

GEORGE TOWN: A secret family password or phrase can help spot scammers as AI voice-cloning technology has become increasingly realistic, said Universiti Putra Malaysia Faculty of Computer Science and Information Technology associate professor Dr Nur Izura Udzir.

"Just as banks use security questions, people can also have a password or phrase known only to their family members," she told *theSun*.

She said AI could now produce voices that sound remarkably like real people, copying not just the way they speak but also their tone, accent and emotions.

She said some systems could even mimic breathing patterns, making it difficult for many people to tell the difference between a genuine voice and an AI-generated one.

Nur Izura said although the technology has many legitimate uses in areas such as education, entertainment and customer service, scammers are finding ways to exploit it.

"When the voice sounds exactly like someone we know, we can easily believe it is

coming from a trusted person. Anybody can fall victim to this."

She said voice-cloning tools are becoming cheaper and easier to access, with some available through commercial platforms and others through open-source software.

Nur Izura said scammers do not rely on cloned voices alone as real-time voice-modulating devices are also available, allowing a human caller to alter his voice live during a conversation to sound like someone the victim knows.

"They can also manipulate caller identification systems so that calls appear to come from a family member, friend or someone whose name is already stored in a victim's contact list."

She said the danger increases when scammers create panic by claiming that a loved one has been kidnapped, involved in an accident or detained by authorities.

She added that some scammers are also using AI systems that could respond during conversations, allowing them to interact with victims in real time rather than relying on pre-recorded messages.

Nur Izura warned that people may not even realise their voices have been copied.

"One method involves silent calls, where

callers remain quiet and wait for the recipient to speak first.

"Some algorithms need only three to 10 seconds to capture a person's voice."

She said voice samples could also be obtained from social media videos, livestreams, interviews, podcasts and public talks.

Nur Izura said public figures, politicians, celebrities and others who frequently appear online are more vulnerable because recordings of their voices are often readily available.

She said police have also advised people not to speak immediately when answering calls from unknown numbers and to wait for callers to identify themselves first.

"If somebody claims to be your family member and asks for money or help, hang up and call back using a trusted number," she added.

She also recommended contacting another relative, friend or neighbour to verify the situation, adding that another option is to ask questions that only the real person would be able to answer.

Nur Izura, who is also an active member of Cyber Security Academia Malaysia, is part of a team of researchers from Universiti Sains Islam Malaysia, Universiti Putra Malaysia, Universiti Kebangsaan Malaysia and International Islamic University Malaysia working with the Home Ministry and the Institute of Public Safety to tackle cyber-enabled crimes.