JOINT ADVISORY BY SINGAPORE POLICE FORCE, MONETARY AUTHORITY OF SINGAPORE AND CYBER SECURITY AGENCY OF SINGAPORE

JOINT ADVISORY ON SCAMS INVOLVING DIGITAL MANIPULATION

The Singapore Police Force (SPF), Monetary Authority of Singapore (MAS) and Cyber Security Agency of Singapore (CSA) would like to alert members of the public to scams involving digital manipulation, in which Artificial Intelligence (AI) is allegedly used to create or manipulate synthetic media (i.e. deepfakes).

2 In this scam variant, scammers would impersonate high-ranking executives from companies that the victims work for through the alleged use of digital manipulation, and instruct victims to transfer funds from company accounts. Victims would receive unsolicited WhatsApp messages from scammers claiming to be executives from the company that the victims work for, inviting the victims to join a live-streamed Zoom video call with their high-ranking executives from their companies. It is believed that digital manipulation had been used to alter the appearances of the scammers to impersonate these high-ranking executives. In some cases, the video calls would also involve scammers impersonating MAS officials and/or potential "investors". Victims would be instructed to transfer substantial amounts of funds from their company's corporate bank accounts to designated bank accounts under the pretext of business payments, such as project financing or investments. Some victims were also asked to disclose personal information such as NRIC and passport details.

3 To reinforce the deceit, victims would be directed to contact a second scammer impersonating as the legal counsels of victims' company, who would send documents such as a Non-Disclosure Agreement or a Board Letter to the victim's personal email address.

4 Victims would subsequently realise that they had been scammed when the scammers become uncontactable, or upon verifying with the actual company's executives and legal counsel, who would confirm that they neither participated in any video calls nor authorised any fund transfers.

5 Businesses are advised to adopt the following precautionary measures:

a. Establish protocols for employees to verify the authenticity of any video calls or messages, particularly those purportedly from senior executives or key stakeholders. Train employees to be vigilant about unsolicited video calls or messages, even if they appear to come from known business contacts.

b. Be mindful of any sudden or urgent fund transfer instructions and verify the authenticity of the instructions with the relevant departments or personnels directly through established communication channels.

c. Analyse the audio-visual elements of the video call. Check for tell-tale signs that could suggest the manipulation of the audio or video through AI technology. For more information, please refer to d**etails in Annex A**. You may also refer to CSA's advisory at https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2024-006

d. Never disclose confidential or personal information or send money to any unknown persons.

e. Alert your employees to this scam, especially those that are responsible for making fund transfers.

f. If you suspect that your company has fallen victim to a scam, call the associated bank immediately to report and block any fraudulent transactions as well as make a police report.

6 MAS would like to alert members of the public that MAS will not, at any time, ask you to transfer money or disclose personal or banking credentials. MAS also does not maintain records of individuals' financial or banking accounts, nor does it hold funds of individuals.

7 If you or your employees are in doubt, call the 24/7 ScamShield Helpline at 1799 to check. For more information on scams, members of the public can visit www.scamshield.gov.sg. Fighting scams is a community effort. Together, we can *ACT* Against Scams to safeguard our community!

SINGAPORE POLICE FORCE
MONETARY AUTHORITY OF SINGAPORE
CYBER SECURITY AGENCY OF SINGAPORE
12 MARCH 2025

Annex A

Screenshots

Tell-tale signs of Manipulated Audio/Video

Multimedia Types	Audio-visual Elements	Description
Images and videos	Facial features	• Blurring around edges of the face, facial features, or the side profile • Uneven resolution and unnatural shadows around facial features • Unnatural edges around features
	Expression & eye movement	• Unnatural or lack of blinking • Inconsistent light reflection in eyes • Unnatural facial expression
	Skin texture & skin tone	• Unnatural or inconsistent skin colour tone • Differences in resolution and skin textures
	Background consistency	• Blurred, out of focus, or distorted areas in the background
Audio and videos	Audio-video consistency	• Lips not synchronised with speech • Limited variance in tone inflection • Incongruent background noise

Source: www.csa.gov.sg/alerts-and-advisories/advisories/ad-2024-006