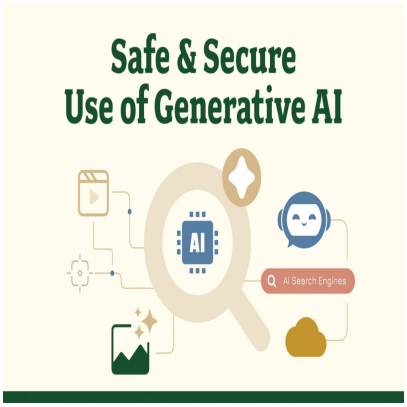

Deepfake Video Call Scam: A Singapore Verification Plan

Description

If a familiar face or voice on a call asks for money, credentials, secrecy or urgent action, stop the transaction and leave the call. Contact the person or organisation through a number, account or colleague you already trust, and verify the request and destination separately. Visual realism is not proof of identity. SPF advisory on manipulated video conference footage. CSAâ??IMDA generative-AI advisory. ScamShield immediate-response guide.

Choose the branch that matches the case

Situation	Next step
No money or credentials have been sent	End the call, preserve the invitation and verify through a known channel
A transfer is queued but not complete	Cancel or freeze it through the bankâ??s official channel immediately
Money or account access was already exposed	Use the bankâ??s emergency route and ScamShieldâ??s current post-scam steps without delay
The caller claims to be a government official	Do not transfer funds or disclose credentials; verify with the named agency independently

What the official record establishes

- SPF advisory on manipulated video conference footage: SPF documents an impersonation video conference, manipulated audio and video, urgent-transfer tactics, visible warning signs and independent verification.
- CSAâ??IMDA generative-AI advisory: The joint advisory covers AI-generated misinformation, official-source verification, sensitive information, permissions and human critical thinking.
- ScamShield immediate-response guide: The official guide provides current steps for people who have transferred money or exposed accounts and identifies the 1799 helpline.

Treat urgency as a control signal

SPFâ??s case involved manipulated footage in a video conference impersonating senior government officials and an urgent request to transfer money. The correct first response is to stop the transaction and verify the identity and request through official sources. SPF advisory on manipulated video conference footage.

Do not stay on the call to prove it is fake. The attacker controls the context, timing and social pressure.

Look for anomalies without relying on them

SPF lists possible audio-visual warning signs such as lip-sync problems, unnatural facial movement and voice or image irregularities. These clues can justify stopping, but a convincing call still needs independent verification. SPF advisory on manipulated video conference footage.

Absence of an obvious artefact is not a pass. Deepfake quality and compression can hide visible defects.

Protect the verification channel

CSA and IMDA advise checking important AI-related information against reliable official sources and limiting sensitive data and permissions. Use a phone number, directory, internal contact or official account obtained before the incidentâ??not a number supplied inside the call. CSAâ??IMDA generative-AI advisory.

Ask the real person to confirm the request, amount, payee and reason. A vague â??yes, it was meâ?• is not enough when money or access is at stake.

Use a two-person transfer rule

For a workplace payment, require a second authorised reviewer to check the invoice, beneficiary, bank and business purpose outside the meeting. For a household transfer, ask a trusted person to repeat the verification steps.

A second person is useful only if they use independent evidence rather than the same forwarded message or call link.

Preserve evidence after leaving

Save the invitation, account name, beneficiary details, timestamps, messages and a description of what appeared unusual. SPFâ??s advisory stresses verification and reporting rather than continuing the suspicious interaction. SPF advisory on manipulated video conference footage.

Do not repost the manipulated clip with exposed names or account details. Preserve it securely for the bank, platform or police route.

Write a challenge that cannot be rehearsed

Ask the real contact through a known channel about a current, non-sensitive fact and require them to restate the exact transaction purpose. Avoid security questions whose answers are public or already disclosed in the compromised call.

The challenge is not biometric proof. It is one layer in a process that also checks the request and destination.

Verify the payee as a separate object

Even after confirming a colleague or relative, compare the destination account with a trusted record. An attacker can mix a real voice, a compromised account and a substituted beneficiary.

Read the payee and amount back through the independent channel before approval.

Respond quickly after a loss

If money or account access was already exposed, contact the bank through its official emergency channel and follow ScamShieldâ??s current post-scam steps. The official site lists the 1799 helpline for scam-related assistance. ScamShield immediate-response guide.

Do not wait to finish a technical diagnosis. Account protection and transfer recall take priority over identifying the exact deepfake method.

Run a five-minute drill before it happens

Agree which transactions require callback, who holds the trusted directory, who can freeze a payment and where incident evidence is stored. Test the process with a harmless scenario and record any delay.

A policy that exists only in a document may fail under pressure. The drill should end with a clear owner for the next action.

Work the example before the real decision

A finance employee sees the managing director on a video call asking for a confidential same-day transfer. The face and voice look plausible. The employee ends the call, phones the director on the number already stored in the corporate directory, checks the beneficiary against the approved vendor record and asks a second authorised reviewer to sign off. The request is rejected before money moves.

Checklist

1. Stop the transfer
2. Leave the suspicious call
3. Use a pre-existing contact channel
4. Verify purpose, amount and payee
5. Preserve the invitation and messages
6. Contact the bank immediately after exposure

Mistakes to avoid

- Waiting for a visible glitch
- Calling a number supplied in the meeting
- Verifying the person but not the payee
- Sharing a one-time code to prove identity
- Delaying the bank while analysing the clip

Related next reads

After stop an irreversible transfer and verify the person, request and destination outside the compromised call, a reader can check a suspicious number, link or message, or recognise a parcel-delivery scam.

Questions readers ask

Can a smooth video call still be fake?

Yes. Use independent identity, request and payee checks even when no obvious artefact appears.

Should I challenge the caller on the same call?

Leave first and use a trusted separate channel.

What if money has already moved?

Contact the bank through its official emergency route immediately and use ScamShieldâ??s current post-scam guidance.

Date Created
03/08/2026
Author
vanessakoh