threat level: human

The attack vector you can't patch.

AI Voice-Clone Scams

When a familiar voice asks for money fast, and how to be sure it is really them.

3 sec
of audio can be enough to clone a voice
McAfee, 2023

$25.6M
stolen in one deepfake video call (Arup)
CNN / FT, 2024

0.1%
of people spotted every deepfake in a test
iProov, 2025

SIGNS A VOICE OR VIDEO IS SYNTHETIC

01 Audio that sounds slightly off
Flat emotion, odd pauses, or breathing and background that do not quite fit.

02 It only works one way
They call you but cannot do a clear live video, or quality drops on a hard question.

THE SCAM THAT RIDES IT

03 A family-emergency call
A loved one's voice in crisis, needing money fast and kept secret.

04 An executive on video pushing a transfer
A familiar face requesting an urgent, confidential payment or login.

05 Pressure not to verify
Discouraging a callback, a second approver, or an in-person check.

COMMON VOICE-CLONE SETUPS

06 The grandparent or child call
A relative 'in trouble', needing money now and begging you to keep it quiet.

07 The boss or finance call
A familiar voice directing an urgent wire or a change to payment details.

08 The bank 'fraud team' call
A caller using a trusted name to move your money 'somewhere safe'.

DO / DON'T

DO

- Hang up and call the real person or organization back on a number you already have.
- Agree on a private code word with family and your finance team.
- Ask a question only the real person would know the answer to.
- Confirm any payment in writing through your normal system.

DON'T

- Do not trust a voice alone. Seconds of audio are enough to clone one.
- Do not act on an urgent money request made only by phone.
- Do not let panic or secrecy stop you from calling back.
- Do not move money 'to keep it safe' on a caller's instruction.

THE ONE MOVE

Hang up and call the real person back on a number you already have, and agree on a private code word with family for emergencies. A few seconds of audio is enough to clone a voice, so trust the callback, not the voice.

IF IT HAPPENS

1. Pause and verify with the real person on a number you choose.
2. If money moved, call your bank immediately to try to recall it.
3. Warn the family member or colleague whose voice was used.
4. Report to ic3.gov and the FTC at reportfraud.ftc.gov.

Get a briefing like this every week, free.

threatlevelhuman.substack.com

youtube.com/@threatlevelhuman

Sources: McAfee (2023); iProov (2025); Hong Kong police / Arup, reported by CNN and FT (2024). Figures as publicly reported.

How this is made: threat level: human is an AI-assisted production. A real person researches every story, checks each claim against primary sources, and is accountable for the facts.