threat level: human

The attack vector you can't patch.

Deepfake Red Flags

A focused guide to spotting AI-generated video and voice, and the scams that ride them.

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

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

$40B
projected US AI-enabled fraud by 2027, from $12.3B in 2023
Deloitte, 2024

SIGNS THE VIDEO OR VOICE IS SYNTHETIC

01 Audio and video that drift
Lip-sync that lags, odd blinking, flat lighting, or a voice that sounds slightly off.

02 Camera or mic problems on cue
They will not turn on a clear camera, or quality drops the moment you ask a hard question.

REQUESTS THAT SHOULD MAKE YOU STOP

03 Urgency on a live call
A senior leader on video pressing for an immediate, secret transfer or login.

04 A request that skips process
Approve now, the usual approver is away, keep this between us.

05 New payment details by voice or video
Bank or wallet changes pushed in a call, never entered in the system of record.

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

07 Context that does not fit
An executive contacting you directly for something they would normally delegate.

THE ONE MOVE

The one move that beats a deepfake: hang up and verify on a channel you chose. Call the person back on a known number, confirm in your finance system, or check in person. A real executive will not punish a callback. An attacker cannot survive one.

Get a briefing like this every week, free.

threatlevelhuman.substack.com

youtube.com/@threatlevelhuman

Sources: Hong Kong police / Arup (reported by CNN, FT), 2024; iProov, 2025; Deloitte Center for Financial Services, 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.