

Deepfakes

AI can clone a voice from 30 seconds of audio and put a fake face on a live video call. Here is what your team needs to know, and the one habit that stops it.

WHAT IT IS

A deepfake is AI-generated audio or video that convincingly imitates a real person. Criminals use it to impersonate your CFO, a supplier or a colleague and authorise payments that should never happen. It is no longer a celebrity problem. It is a finance problem, and any organisation that moves money is a target.

WHY IT MATTERS

\$410M

Reported deepfake-fraud losses in the first half of 2025, more than all of 2024.

Surfshark, 2025

20–30s

Of audio is enough to clone a usable voice.

World Economic Forum, 2025

45 min

To build a convincing video fake with free tools.

World Economic Forum, 2025

WHAT HAPPENED

In 2024 a finance worker at engineering firm Arup paid out about 25 million dollars after a video call where the CFO and colleagues were all real-time deepfakes, built from public footage. The same trick hit WPP and Ferrari and failed, because in each case one person paused and verified through a separate channel. (CNN, 2024)

RED FLAGS TO WATCH FOR

You cannot reliably spot a deepfake by eye, so watch the behaviour, not the face.

- Urgency and secrecy, a confidential deal that supposedly cannot wait.
- Pressure to skip the normal payment or sign-off process.
- A request through an unusual channel, like WhatsApp or a surprise video call.
- Reluctance to switch to a known number or to do a callback.

Verify every unusual or high-value request through a second, known channel before acting. Never through the channel the request arrived on.

THEN BUILD THE HABIT AROUND IT

- Require two people to authorise payments above a set amount.
- Agree a verification question or code word for sensitive requests.
- Confirm supplier bank-detail changes on a number you already hold.
- Treat no payment as too urgent or too secret for normal verification.

MYTHS AND FACTS

MYTH I can spot a deepfake if I look closely enough.

FACT Real-time fakes pass visual inspection. The people fooled at Arup were looking at familiar faces. Verification, not your eyes, is the control.

MYTH A live video call proves the person is real.

FACT At Arup everyone on the call except the victim was fake. A call is just a channel, and channels can be faked.

MYTH This is a problem for IT to solve.

FACT It targets finance, HR and payment approvers. The fix is a verification habit those teams own and use.

THE LEGAL DUTY

Security awareness training is now a legal duty under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, with boards personally accountable under Article 20.

GET HELP

eBuilder Security runs Sweden-based security awareness and phishing-simulation training that builds exactly this verification habit. Read the full guide at the link below.

[Read the Full Article →](#)