

AI-Powered Social Engineering

AI now writes flawless phishing, clones a voice from seconds of audio and fakes live video calls. Here is what your team needs to know, and the one habit that stops it.

WHAT IT IS

AI-powered social engineering is the use of artificial intelligence to manipulate people into sending money, sharing credentials or granting access. Attackers use generative AI to write convincing phishing, clone voices and fake live video calls, so the old warning signs of a scam mostly disappear. It is a finance and access problem, and any organisation that moves money is a target.

WHY IT MATTERS

2.77 billion dollars

Reported US losses to business email compromise in 2024, the executive-impersonation scam AI makes easier.

FBI IC3, 2024

54 percent

Click-through for AI-written spear-phishing in a controlled study, matching human experts against 12 percent for generic phishing.

Heiding et al., 2024

A few seconds

Of recorded audio can be enough to clone a usable voice.

FBI, 2024

WHAT HAPPENED

In 2024 a finance worker at Arup's Hong Kong office paid out about 25 million dollars after joining a video call on which the CFO and colleagues were all real-time deepfakes, built from public footage. He had first suspected a phishing email, but the familiar faces overrode his doubt, and he only realised after checking with head office. (CNN, citing Hong Kong police, 2024)

RED FLAGS TO WATCH FOR

You cannot reliably spot a modern fake by eye or ear, so watch the behaviour, not the face or voice.

- Urgency and secrecy, a request that cannot wait and must stay confidential.
- An unusual channel, a boss or supplier suddenly on WhatsApp or a surprise video call.
- Pressure to skip the normal payment or sign-off process just this once.
- A nudge to move the conversation to a different or encrypted app.

THE ONE RULE THAT STOPS IT

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 and bank-detail changes above a set amount.
- Agree a call-back protocol, confirming requests on a number already on file.

- Set a code word or challenge question for sensitive requests, as Ferrari's executive used.
- Run regular awareness training and phishing simulations so staff practise it.

MYTHS AND FACTS

MYTH

A live video or voice call proves the person is real.

FACT

At Arup every colleague on the call was a deepfake. A call is only a channel, and channels can be faked.

MYTH

AI phishing is easy to spot because scam emails are badly written.

FACT

That tell is gone. AI now writes fluent and personalised messages that match human experts for click-through.

MYTH

This only targets big corporations.

FACT

AI lowers the cost of each attack, so small and mid-sized organisations are targets too.

THE LEGAL DUTY

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

[Read the Full Article →](#)