

AI-Powered Phishing

Generative AI now writes flawless scam emails and can clone a voice or a face for a live call. Here is what your team needs to know, and the one habit that stops it.

WHAT IT IS

AI-powered phishing is a phishing attack that uses artificial intelligence to make the deception convincing. Criminals use it to write fluent tailored emails, clone an executive's voice or fake a face on a video call, then push a payment or a login that should never happen. The old advice to watch for bad spelling no longer protects anyone.

WHY IT MATTERS

2.9 billion dollars

Reported US business email compromise losses in 2023, the fraud AI phishing feeds.

FBI IC3, 2023

Most reported

Phishing is the most reported cybercrime complaint in the United States.

FBI IC3, 2023

Harder to detect

AI's assessed effect on phishing over 2024 to 2025.

UK NCSC, 2024

WHAT HAPPENED

In early 2024 a finance employee at engineering firm Arup joined a video call where the CFO and colleagues were all real-time deepfakes built from public footage. They authorised transfers of about 25 million US dollars. Similar attacks on Ferrari and WPP the same year failed, because in each case someone paused and verified through a separate channel. (Hong Kong police, 2024)

RED FLAGS TO WATCH FOR

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

- Urgency and secrecy, a deal that supposedly cannot wait and must stay quiet.
- Pressure to skip the normal payment or approval steps.
- A first approach through an unusual channel, like WhatsApp or a surprise video call.
- A change of bank details or a new payee sent by message.
- Reluctance to move to a known number or an official channel.

THE ONE RULE THAT STOPS IT

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

THEN BUILD THE HABIT AROUND IT

- Require two people to approve payments above a set amount.

- Agree a verification word or question for sensitive requests.
- Confirm supplier bank-detail changes on a number you already hold.
- Turn on phishing-resistant multi-factor authentication for email and key systems.

MYTHS AND FACTS

MYTH

I can spot an AI phishing email because the writing is bad.

FACT

Generative AI writes fluent error-free messages. Clean writing is no longer a sign that a message is safe.

MYTH

A phone or video call proves the person is real.

FACT

Voices and faces can be cloned in real time. A call only proves the channel, so verify another way.

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 and incident handling are legal duties 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 →](#)