

AI Security Awareness Training

AI now writes flawless phishing, clones a voice from a short clip and puts a fake face on a live video call. Your people are the target and the tools they use are part of the risk. Here is what to train them on and the single habit that holds.

WHAT IT IS

AI security awareness training teaches staff to recognise attacks that use artificial intelligence and to use AI tools safely without leaking data. It is the modern form of security awareness training, rebuilt for a year when a convincing fake of your CFO can appear on a video call. Any organisation that moves money or handles sensitive data is a target.

WHY IT MATTERS

22,364

US fraud complaints referencing AI in 2025, with about 893 million dollars in reported losses.

FBI IC3, 2025

47%

Of organisations name AI-powered attacks as their top cyber concern.

World Economic Forum, 2025

about 2%

Cut in phishing clicks from standard awareness training, in a controlled study of 19,500 staff.

UC San Diego, 2025

WHAT HAPPENED

In January 2024 a finance worker at engineering firm Arup paid out about 25.6 million dollars after a video call where the CFO and colleagues were all real-time deepfakes, built from public footage. The fraud was caught only after the money had gone, and it was never recovered. (Hong Kong police, CNN, 2024)

RED FLAGS TO WATCH FOR

You cannot reliably spot a good fake by eye, so watch the behaviour rather than the face.

- Urgency and secrecy, a confidential request that supposedly cannot wait.
- Pressure to skip the normal payment or sign-off process.
- A request through an unusual channel, such as a personal chat app or a surprise video call.
- A changed bank detail or a reluctance to move to a number you already hold.

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 authorise payments above a set amount.
- Agree a code word or verification step for sensitive requests.

- Confirm any change to supplier bank details on a number you already hold.
- Give staff an approved AI tool and a clear rule on what must never be entered.

MYTHS AND FACTS

MYTH

One annual training course keeps us covered.

FACT

A 2025 study of 19,500 staff found annual training had no significant effect on how often people fell for phishing. Short, frequent and role-based training works better.

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 only a channel, and channels can be faked.

MYTH

Banning AI tools removes the data risk.

FACT

Staff route around bans, as they did at Samsung in 2023. Give them a sanctioned tool and a clear rule instead.

THE LEGAL DUTY

AI literacy has been a legal duty under the EU AI Act since 2 February 2025. NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, also requires security awareness training, with boards personally accountable.

GET HELP

eBuilder Security runs employee cybersecurity training built around these AI threats, so your team learns to verify before it acts. Read the full guide at the link below.

[Read the Full Article →](#)