



Too real to be true?

Recognising AI-driven scams in a world where trust is under attack

Artificial intelligence is changing the way we live and work. But it's also giving scammers new tools to trick us. From fake voices that sound exactly like our loved ones to convincing videos of someone saying things they never said, AI-driven scams are becoming harder to detect. These scams prey on our emotions and trust, using manipulative tactics to influence or pressure us.

How does it work?

AI-powered scams build on the **same psychological tricks** scammers have always used. Their goal still is to trick you into doing something you normally wouldn't do, like clicking a malicious link, sharing sensitive information, or transferring money. What's changed is **how easy it has become for them to sound and look convincing**.

Here are some common types of AI scams:

Deepfake impersonations

Scammers use AI to create realistic audio or video of a trusted person - your boss, partner or even your child - to pressure you into sending money, sharing credentials, or clicking a malicious link. These impersonations can happen in video calls, voicemails or social media messages.

Voice cloning phone scams

Criminals use AI to clone voices from short audio samples (like a voicemail or YouTube clip). With just a few seconds of audio, they can make a call that sounds eerily familiar and urgent.

Romance and relationship scams

Chatbots pretending to be real people build relationships over time, slowly gaining your trust and personal details before asking for money or favours.

Business email compromise

AI makes it easier to craft highly targeted phishing emails that appear to come from someone inside your organisation, often combined with deepfake calls or voice messages.

Mass-scale scam calls and messages

AI allows criminals to send thousands of customised messages or calls at once, all personalised with information they've found online or through data leaks.

Investment scams

AI is used to create fake slick-looking websites, fake news, or fake endorsements that make scams look legitimate, especially around crypto or “too good to be true” opportunities.

Spot the signs

AI-driven scams are designed to feel real. Here are a few red flags to watch out for:

- **Unusual behaviour:** Someone you know is communicating in a strange way: their tone feels off, the language seems unusual, or their requests don't make sense.
- **Emotional manipulation or urgency:** You're told to act immediately or face serious consequences. Scammers often use fear, love, or excitement to cloud your judgment.
- **Channel switching:** You're pushed to move the conversation to another platform (e.g. from email to WhatsApp) quickly.
- **Too-perfect profiles:** Online profiles seem overly polished, with little interaction history or stock photos or images that can be found elsewhere online - often not matching the person's claimed identity.

Remember: It's not about spotting the “fake video”, it's about **spotting suspicious situations**.

What can you do?

- **Pause and breathe.** Scams are designed to make you act fast. Slowing down gives your brain time to spot red flags.
- **Always verify.** Especially when someone asks you to do something unexpected. Use another channel to confirm if the request is genuine. If someone asks for money, data or urgent action, confirm their identity via a separate communication method (e.g. call their known number).
- **Use a code word.** Share a "safe word" with family or colleagues to confirm it's really them. Check our one-pager about the use of code words.
- **Don't share too much online.** Scammers gather personal details from social media to personalise their attacks.
- **Be mindful of new connections.** Take your time with new online relationships or people asking for help.
- **Report and get help.** If something feels off or if you're unsure, contact your IT team or security officer. In a private context, reach out to the relevant authorities or your national cyber support service.

Be mindful. Stay safe.

AI scams aren't just about technology, they're about **psychology**. Stay mindful, pause before reacting, and remember: it's ok to double-check. In a world full of digital illusions, digital mindfulness is your strongest defense.

Learn more

- 🔗 [Deepfakes when video evidence lies](#) (source: iBarry)
- 🔗 [ENISA Threat Landscape 2024](#) (source: ENISA)
- 🔗 [Facing Reality: Law Enforcement and the Challenge of Deepfakes](#) (source: Europol)
- 🔗 [Impact of AI on cyber threat from now to 2027](#) (source: NCSC UK)

BE MINDFUL. STAY SAFE.

