THE AI SCAM CHECKLIST

Is it real? 12 calm checks to spot AI scams

A plain-English guide for the UK, for anyone new to AI and the people who look out for them.

Scammers now use AI tools to copy voices, make fake videos of famous people and write messages with perfect spelling. That sounds worrying, but the good news is simple: **the same few habits still protect you.** You don't need to be good with technology to use them.

Your three-step routine: Stop. Check. Call.

1

Stop

Don't act straight away. A real bank, company or loved one will understand if you take a few minutes.

2

Check

Use the checks in this guide. Ask yourself: could this be fake? It's fine to say no or ignore it.

3

Call

Ring back on a number *you* already trust, never one given in the call, text or email.

Good to know: this fits with the UK's national Take Five advice, "Stop, Challenge, Protect". Only criminals will try to rush or panic you.

How to use this guide: print it and keep it by the phone, go through it with family, or pass it on to a friend. Each check takes only a moment.

The 12 checks (part 1)

Tick each one off in your head when something feels unusual.

"Family emergency" calls with a copied voice

1 Are you being rushed, or told to keep it secret?

AI can copy a voice from a short online clip. If "your grandson" needs money urgently and says "don't tell Mum", that's a warning sign, even if the voice sounds exactly right.

2 Have you hung up and rung them back yourself?

Call the person on the number saved in your phone, or ring another family member. Ask for your family safe word (see page 3).

Fake celebrity investment adverts

3 Is a famous face promising easy money?

Videos and photos of well-known people can be faked with AI. Treat any advert where a celebrity promises big or "guaranteed" returns as fake.

4 Have you checked the firm with the FCA?

Before investing, look the firm up with the Financial Conduct Authority's Firm Checker at **fca.org.uk**, or call the FCA on **0800 111 6768**.

AI-written emails and texts

5 Were you expecting it?

Perfect spelling no longer means a message is genuine. Be wary of any message you weren't expecting that asks you to click, pay, log in or "confirm your details".

6 Have you gone to the website or app yourself?

Don't use the link or phone number in the message. Type the web address you know, or open the company's official app.

The 12 checks (part 2)

Fake chatbots and customer service

7 Did you find the contact details yourself?

Fake "help" chats, adverts and social media accounts can look official. Use contact details from the company's own website, your statement, or the back of your card.

8 Are they asking for your PIN, password or a code?

Never share these, or the one-time code sent to your phone. Never install an app that lets a stranger control your computer or phone.

Romance scams

9 Has someone you've never met asked for money?

Even after weeks of kind messages, never send money or gift cards to someone you haven't met in person, whatever the reason.

10 Have you talked it over with someone you trust?

Photos, videos and even video calls can be faked. A friend or relative can often spot what's hard to see from the inside.

QR code scams

11 Is the QR code a sticker on top of another?

On car park machines and posters, a fake code can be stuck over the real one. If in doubt, use the official app or pay at the machine.

12 Have you checked where it takes you?

Treat a QR code like a link. Look at the web address before entering any details, especially if it came in an unexpected letter, email or text.

Tip: agree a family safe word

Choose a word or short phrase with your close family that a stranger couldn't guess, and that's never posted online. If someone calls in a panic asking for money, ask for the safe word. No word, no money, and ring them back on their usual number.

If you think you've been caught out

Please don't feel embarrassed: these scams are made to fool careful people. Acting quickly helps.

1. **Stop** sending money or sharing information.
2. **Call your bank straight away** on the number on the back of your card, or dial **159**.
3. **Change your passwords** for any affected accounts and turn on 2-step verification.
4. **Keep evidence**: messages, screenshots, phone numbers, web addresses and payment details.
5. **Report it** using the contacts below.
6. **Watch for follow-up scams.** Never pay anyone who offers to "recover" your money for a fee.

Who to contact in the UK

Your bank	**Number on the back of your card**, or dial **159** to be put through to your bank. 159 will never call you.
Report Fraud (replaced Action Fraud)	England, Wales & N. Ireland: **reportfraud.police.uk** (any time) or **0300 123 2040** (Mon–Fri, 8am–8pm)
In Scotland	Police Scotland on **101**
Scam text messages	Forward the text to **7726** (free). For a scam call, text "Call" and the number to 7726.
Scam emails	Forward to **report@phishing.gov.uk**
Scam adverts online	Report to the Advertising Standards Authority at **asa.org.uk**
In danger right now	Call **999**

Want to use AI safely and confidently?

Our AI Basics course is a calm, plain-English start for beginners:
aiessential.ai/ai-basics
Questions? Email us at **hello@aiessential.ai**