

Staying safe from AI scams

Recognize the scams AI makes easier, like fake invoices, convincing emails and cloned voices, and know what to do next.

Try it

- 1 **Spot the signs.** Read this email and pick out what feels wrong:

URGENT: We have changed our bank details. Please pay invoice 2231 (£1,480) to our new account today to avoid late fees.

- 2 **Ask AI for a second opinion.** Take out any names and account numbers first, then paste a suspicious message and ask:

What signs suggest this message might be a scam?

AI can point out warning signs. It can't tell you a message is safe.

- 3 **Your callback habit.** Pick one supplier. Write down their phone number from an old invoice or their website, not from a new email. That's the number you call to check any change.
- 4 **A safe question.** Voices can now be copied. Agree a question with family or staff that only you would know, for any urgent call asking for money.

Where to report

Suspicious email

forward it to report@phishing.gov.uk

Scam text

forward it to 7726

A call "from your bank"

hang up, then call 159

Lost money

call your bank straight away, then Report Fraud: reportfraud.police.uk or 0300 123 2040

TAKE-HOME RULE

Changed bank details? Call the number you already have.