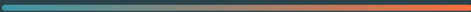


AI FOR EVERYONE

# How to spot an AI scam (a plain guide for you or someone you love)

Scammers now use AI to clone voices and write convincing messages. Here is how to spot them, in plain English — and one rule that stops almost all of them.

  
**For everyone** Shipped — measured, gate-clean

COVER: A CALM DAWN · A WARM, HUMAN ILLUSTRATION

# How to spot an AI scam (a plain guide for you or someone you love)

Scammers now use AI to clone voices and write convincing messages. Here is how to spot them, in plain English — and one rule that stops almost all of them.

---

## 01 Start here

---

## 02 What AI actually changed

---

## 03 The three things every scam needs

---

## 04 The AI voice-cloning call

---

## 05 Messages, emails and "your parcel is waiting"

---

## 06 If you think you've already been caught

---

## 07 Sources, glossary & the honesty ledger

Every claim carries its tier · nothing faked

---

### PREPARED

20 June 2026

### VERIFIED BY

Jon Ross — Founder, Vocabotics —  
15 years building safety-critical AI

### HOW TO READ IT

Drafted with AI, verified by a  
named human. Sources at the back.

# 01 Start here



If you have had a message that felt urgent and a little bit *off* — a call from a grandchild in trouble, a text from your bank, an email about a parcel — you are right to pause. Scammers now use AI to sound more convincing than ever. The good news: the tricks are old, only the polish is new. Once you know the shape of them, they are easier to spot, not harder.

## You are not being paranoid.

Being careful is not being rude. A real bank, a real family member, and a real company will all understand completely if you hang up and call them back on a number you already trust. Anyone who *won't* let you do that is the problem.

# 02 What AI actually changed



For years, you could spot a scam by the clumsy spelling and the odd phrasing. AI has taken that clue away. A scam email can now be word-perfect. Worse, AI can copy a voice from a few seconds of audio — a video online, a voicemail greeting — and use it to make a call that sounds like someone you know.

So the old advice ("watch for bad spelling") no longer works on its own. The advice that still works is about **what they ask you to do**, not how polished they sound.

# 03 The three things every scam needs



Almost every scam — AI-powered or not — leans on the same three levers. If you see two or three of them together, treat it as a scam until you've proven otherwise.

**Urgency.** "Act now." "Your account will be closed." "I'm in trouble and I need it in the next hour." Urgency is designed to stop you thinking.

**A change to how money or details move.** A new bank account to pay into. A gift-card code. A request for a password, a PIN, or a one-time security code.

**A reason you can't check right now.** "Don't tell anyone." "I've lost my phone, this is my new number." "The line is bad." They need to keep you from calling the real person.

### The one rule that stops almost all of them

**Hang up, then check on a number you already have.** Not the number that called you. Not a link in the message. Call your bank on the number on your card, or call your family member on the number in your contacts. A real emergency survives a five-minute call-back. A scam does not.



#### Urgency

'act now or lose it' — a pressure to skip checks



#### A trusted mask

your bank, a parcel firm, a family voice



#### A payment or code

money, a login, or a one-time code

*Every scam needs the same three things. Break any one and the scam fails — which is exactly how you stop it.*

## 04 The AI voice-cloning call



This is the one worrying families most, so let's be specific. You get a call. It sounds like your son, your daughter, your grandchild. They're upset. They've had an accident, or they're in trouble abroad, and they need money fast — and please don't tell Mum.

Here is what to do, calmly:

Say you'll call them straight back, and hang up.

Call them on the number you already have saved.

If you can't reach them, call another family member who can.

Agree a **family safe-word** in advance — a simple word only you know. If a panicked call can't give the word, it isn't them.

The voice may be perfect. The story will still fall apart the moment you check it against reality.

**Are they rushing you to pay or share a code?**

**Yes** → Stop — that pressure is the tell

**No** → Still verify who they are

**Can you reach them on a number YOU already have?**

**Yes** → Hang up and call it to check

**No** → Do not act until you can

**Do they ask for a code, password or bank move?**

**Yes** → No genuine caller ever needs this

**No** → Confirm before doing anything

*The calm test for a panicked call or message — one question defeats a cloned voice.*

## 05 Messages, emails and "your parcel is waiting"

**F**or texts and emails, the same rule applies: don't tap the link. Go to the company yourself — type the address you know, or use the app you already have.

Banks will **never** ask you to move money to a "safe account". That instruction is always a scam.

A real delivery company won't need a fee unlocked by clicking a link in a text.

If an email address or web address is *almost* right but slightly wrong, that's a red flag, not a typo.

*If you think you've been targeted, report it — reporting helps stop the same scam reaching someone else.*

Report a scam · gov.uk · as of June 2026

## 06 If you think you've already been caught

**F**irst, breathe. It happens to careful, intelligent people every day — that's the whole point of the trick. Then:

Call your bank straight away on the number on your card and tell them.

Change any password you gave away, and any you reused elsewhere.

Report it (in the UK, Action Fraud; in the US, the FTC — links below).

Tell someone. Scammers rely on shame to keep you quiet. Talking about it protects the next person.

You did nothing stupid. You were targeted by people who do this all day. Knowing the shape of the trick is most of the defence — and now you do.

## 07 Sources, glossary & the ledger

Where every claim comes from — and what the plain words mean.

---

### Sources

- 01 **Recognise and report scams** — UK National Cyber Security Centre (as of June 2026)  
<https://www.ncsc.gov.uk/collection/phishing-scams>
- 02 **How to spot a scam** — Action Fraud (UK) (as of June 2026)  
<https://www.actionfraud.police.uk/>
- 03 **Scams and how to avoid them** — US Federal Trade Commission (as of June 2026)  
<https://consumer.ftc.gov/scams>

#### THE HONESTY LEDGER

- Shipped — measured, gate-clean.
- 🔬 Research — measured, partial; the gap is shown.
- 🔭 Vision — designed, honest; not yet built.

The bigger claim goes up a tier, never down. We show the eval beside the demo — the tiering is the credibility.

---

## Share this with one person who'd find it useful

The best protection is a quick chat before money moves. Send this to a parent, a grandparent, or a friend — and browse the rest of the AI-for-everyone guides.

</resources/ai-for-everyone>

---

---

## Nothing faked.

Drafted with AI and verified by a named human. No jargon, no selling, no affiliate links — just what is honestly true about AI for an ordinary person.

