FREE PRINTABLE GUIDE

PLAIN ENGLISH
SAFETY GUIDE



Spot AI Scams

Spot the signs. Protect your family. Know what to do.

5 warning signs | 5 scams to know | Fridge card

SimplyAI Club

simplyaiclub.com

Spot AI Scams: a free SimplyAI Club guide

Version 4, November 2026

Copyright © 2026 Suky Singh, SimplyAI Club. All rights reserved.

Sharing. This guide is free. You are welcome to print it and share it, unchanged and free of charge, with family, friends and community groups. You may not sell it or present it as your own.

Disclaimer. This guide is for general information and education only. It is not legal, financial, security or other professional advice. Scams and reporting services change; contact details were checked on 22 November 2026. If you think you have been scammed, contact your bank and the official services listed straight away. The author accepts no liability for any loss arising from use of this guide.

Examples. The calls and messages in the examples are illustrative and not real.

Trademarks. All product and company names are trademarks of their respective owners and are used only to identify them. This guide is independent and not endorsed by any of these organisations.

Links. Links and QR codes to third party websites are provided for convenience. The author is not responsible for the content of those sites.

All icons and illustrations are original to this guide.

Contents

Section	What you will find	Page
Welcome	How to use this guide, and why scams feel different now	3
The five warning signs	The signs that never change	4
Five AI scams to know	What each looks like and what to do	5
Two real examples	A cloned voice and a parcel text	7
A family code word	An extra check, never proof	8
Stop. Check. Protect.	Your 60 second check	9
If you already clicked or paid	What to do next, step by step	10
Who to contact	UK and US reporting contacts	11
Printable fridge card	Cut out and keep by your phone	12
Sources	Where the facts come from	13
About the author	Who wrote this guide, and where to learn more	14

Tip: in the PDF, click any section name to jump straight to it.

STOP. CHECK. PROTECT.

Stop before you act. Check on a number you trust. Protect your money and details.

Welcome

Scammers now use AI to sound more convincing. A few simple checks can help you spot and avoid them, and this guide shows you those checks in plain English. You do not need to understand how AI works.

How to use this guide

This free guide takes about 15 minutes to read.

- **Read it once,** ideally with a family member. Ten minutes over a cup of tea is enough.
- **Talk about the checks** with the people you love, especially Stop, Check, Protect.
- **Print the fridge card** and keep it by your phone.

UK and US contact details in this guide were checked against official sources on 22 November 2026. Services change, so check the official websites if in doubt.

Why scams feel different now

The old clues, like poor spelling or a stranger's voice, are no longer reliable. AI tools let scammers do three things cheaply:

1. **Write convincing messages** with few or no obvious mistakes. Emails and texts can read like they came from your bank, a delivery company or a government office.
2. **Copy a voice.** A short clip of someone's voice, taken from a video posted online, can be enough to make a call sound just like them.
3. **Fake a face.** Videos and photos of famous people can be made to say things they never said, often to sell "investments".

The good news

AI changes how a scam looks, not what it wants. Almost every scam still needs you to act fast, keep it secret, or hand over money or details. That is how you catch it.

The five warning signs

If a message or call shows even one of these signs, stop and check before you do anything.



Hurry

"You must act now", "Your account closes today", "I need it in the next hour"



Secrecy

"Don't tell anyone", "Don't call the bank, they are part of it"



Strange ways to pay

Gift cards, cryptocurrency, a bank transfer to a "safe account", or cash collected from your door



Codes or passwords

"Read me the code we just sent you", "Confirm your PIN"



Out of the blue

A call, text or advert you did not expect, offering a prize, refund or investment

Remember: your bank, the police and government offices will never ask you to move money to keep it safe, or to tell them a PIN or a password.

Five AI scams to know

1. The call that sounds like family

A panicked voice that sounds exactly like your son, daughter or grandchild says they are in trouble and need money now. The voice may be a copy made with AI.

What to do

Hang up, even if the voice sounds real. Call them back on a number you already have saved, or call another family member, before you send anything.

2. The convincing email or text

A message from your "bank", a parcel company, HMRC or a streaming service says there is a problem and gives you a link to fix it. AI helps these messages look professional.

What to do

Do not click the link or call the number in the message. Open the company's own app or website yourself, or call the number on the back of your card.

3. The famous face selling an investment

A video or advert shows a well known person, perhaps a TV presenter or business leader, recommending a way to get rich quickly. These videos can be faked with AI.

What to do

Treat any unexpected celebrity investment endorsement as suspicious. Check the person's official website or accounts, and in the UK check the firm on the Financial Conduct Authority register (register.fca.org.uk) before you pay anything.

4. The caller from your bank or the police

Someone says your account has been hacked and you must move your money to a "safe account", or hand cash or your card to a courier. The number on your screen may even look genuine.

What to do

Hang up. Wait a few minutes or use a different phone, then call your bank on the number you trust. Your bank will never ask you to move money to keep it safe.

5. The fake AI helper

An app, website or message offers a "special" AI assistant, a prize or a refund, and asks you to log in, pay a fee or share personal details.

What to do

Fake apps can appear even in official app stores. Check that the publisher name matches the real company, or follow the download link from the company's own website. Never type passwords or card details into a link someone sent you.

Two real examples

These show how the advice works in practice.

Example 1: the cloned voice

The call: "Mum, I've had an accident. Please send £500. Don't call anyone."

Warning signs: hurry, secrecy, a request for money.

What to do: hang up. Call your son or daughter on the number saved in your phone. Do not send any money until you have spoken to them yourself.

Example 2: the parcel text

The text: "Your parcel cannot be delivered. Pay £1.95 using this link."

Warning signs: out of the blue, a link, a small payment to get your card details.

What to do: do not open the link. If you are expecting a delivery, check it in the retailer's or courier's own app or website.

A family code word

A family code word can give you an extra warning sign, but it is **not proof of identity**. Code words can be overheard, guessed or shared by mistake.

1. **Choose it together, in person.** Pick a word or short phrase that is hard to guess. Avoid pet names, birthdays or anything posted online.
2. **Never write it** in a text, email or social media post.
3. **Let the caller say it first.** If you are unsure, ask "What's our word?" Do not offer it yourself.
4. **Always call back anyway.** If a caller asks for money or urgent help, hang up and call your relative on a number you already know, even if the caller knows the code word.

Stop. Check. Protect.

Your 60 second check. Before you click, pay or share anything, run through these three steps.

STOP	CHECK	PROTECT
Do not click, pay or share any more information.	Contact them on a number or app you already trust, never one they gave you.	Already sent money or details? Call your bank or provider straight away.

Avoid the suspicious request, but do not wait: if money or personal information may already be at risk, contact your bank or provider promptly. If you are not sure, tell someone you trust.

If you already clicked or paid

Act quickly and do not feel embarrassed. Scams fool careful, clever people every day.

Clicking a link on its own does not always mean harm is done. What to do depends on what happened next:

If you…	Do this now
Only opened the link and closed it	Do not enter anything. Delete the message and report it (see Who to contact). Keep an eye on your accounts.
Typed a password on the page	Change that password straight away on the real website or app (type the address yourself). Change it anywhere else you use the same password.
Downloaded an app or file	Do not open it again. Run a scan with trusted security software, and contact your device maker's official support. Deleting the file alone may not remove harmful software. If you entered passwords or gave the app access to your accounts, change your passwords using a trusted device and contact the relevant provider.
Shared bank or card details	Call your bank immediately using the number on your card, or call 159 in the UK.
Sent money	Call your bank immediately. The faster you act, the better the chance of stopping the payment. Then report it.

Make your accounts harder to break into

- **Turn on extra sign in checks.** Many accounts can send a code to your phone or use an authenticator app when you log in.
- **Use passkeys where offered.** A passkey lets you sign in with your fingerprint, face or phone PIN instead of a password, and cannot be typed into a fake website.
- **Watch your statements** for a few weeks for anything you do not recognise.

Who to contact

In the UK

What happened	Who to contact
Money lost or bank details shared	Your bank, or call 159 to be connected to your bank safely
Report the scam to the police (England, Wales and Northern Ireland)	Report Fraud: reportfraud.police.uk or 0300 123 2040
Report the scam in Scotland	Police Scotland on 101
Scam text message	Forward it free to 7726
Scam email	Forward it to report@phishing.gov.uk
You feel in danger	999

Report Fraud replaced Action Fraud in December 2025. The phone number stayed the same.

In the US

What happened	Who to contact
Money lost or bank details shared	Your bank, using the number on your card
Report a scam	ReportFraud.ftc.gov
You feel in danger	911

Printable fridge card

Cut along the border and keep it by your phone. A separate one page version is included with this guide.

SimplyAI Club

STOP

Do not click, pay or share

CHECK

Call back on a number you trust

PROTECT

Already paid or shared? Call your bank now

UK	US
Your bank: 159	Your bank: number on your card
Report Fraud: 0300 123 2040	ReportFraud.ftc.gov
Scam texts: forward to 7726	Emergency: 911
Emergency: 999	

Family code word: remember it, do not write it here

Sources

All accessed 22 November 2026.

- **Ofcom: What to do about a scam call, text or message**
  https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/what-to-do-about-a-scam-call-text-or-message
- **Report Fraud: Report Fraud service goes live**
  https://www.reportfraud.police.uk/news/report-fraud-service-goes-live/
- **City of London Police: Report Fraud service goes live**
  https://www.cityoflondon.police.uk/news/city-of-london/news/2025/december/report-fraud-service-goes-live-with-full-public-launch-in-january-2026/
- **GOV.UK: Avoid and report internet scams and phishing**
  https://www.gov.uk/report-suspicious-emails-websites-phishing/hmrc-scams
- **Age UK: Avoiding scams (insert)**
  https://www.ageuk.org.uk/siteassets/documents/id205939-avoiding-scams-insert.pdf
- **FTC: Scammers use AI to enhance their family emergency schemes**
  https://consumer.ftc.gov/node/80688
- **Scientific American: A safe word can protect against AI impostor scams**
  https://www.scientificamerican.com/article/a-safe-word-can-protect-against-ai-impostor-scams/
- **Financial Conduct Authority: Financial Services Register**
  https://register.fca.org.uk/

About the author

Suky Singh founded and led HSBC's Global FinOps Centre of Excellence, delivering £315M+ in documented cloud savings. After 30 years in enterprise technology, he helps people and businesses understand AI and use it safely and wisely.

He started SimplyAI Club to help everyday people, of any age, feel confident with AI, without technical jargon.

Explaining AI to all is my mission.

Keep learning

More free guides

simplyaiclub.com

AI Made Simple workbook

The beginner's workbook on Gumroad

- **Visit:** simplyaiclub.com for more free beginner resources.
- **Read more:** AI Made Simple, the beginner's workbook, for step by step help using AI with confidence.
- **Get in touch:** hello@simplyaiclub.com

LinkedIn: linkedin.com/in/suky-singh

Thank you

To my wife, Pam, and our children, Mahi and Reece, and to all my friends: thank you for your unwavering support. This guide would not exist without you.

Suky