

A FREE TASTER FROM MONEY: FROM SHELLS TO SCAMS

Spot the Scam!



The 10 biggest red flags, and what to do
if it happens to you

ACT NOW!

I'M FROM YOUR BANK



HI MUM, NEW NUMBER

PAY BY GIFT CARD

STOP. CHECK. CALL 159.



The 10 biggest red flags

Scams aren't a test of how clever you are. They are run by organised criminals who catch people at a busy, worried or hopeful moment. Most scams use the same few tricks. Learn these ten and you'll spot almost any of them.

1

Rush and panic

"Act now or your account will be closed today."

Scammers want you to act before you think: a deadline, a threat, a fine, or "only two left". Fear and hurry switch off the part of your brain that spots a con.

DO THIS Slow down. A real bank, company or council will let you take your time. Hang up or close the message, then check using a number or website you find yourself.

2

"Move your money to a safe account"

"Your account's been hacked. Move your savings now to keep them safe."

A caller says they are your bank, the police or the fraud team, and you must move money to protect it. The "safe account" belongs to the criminals.

DO THIS Stop. There is no such thing. Hang up and call 159 or the number on the back of your card.



Asked to read out a code

“We’ve just texted you a code. Can you read it back to confirm it’s you?”

Those one-time codes approve payments, add your card to someone else’s phone or unlock your WhatsApp. Whoever has the code has the key.

DO THIS Treat every code like your PIN. Never read it out or forward it to anyone, even someone who says they are your bank.



Too good to be true

“Congratulations, you’ve won!” · “iPhone, £120, collection only”

Prizes you never entered, giveaways, rock-bottom prices on marketplaces, sold-out tickets suddenly “available”. The bargain is the bait.

DO THIS If you didn’t enter, you didn’t win. Buy from sellers you can check, and pay by card or a platform’s own checkout, not bank transfer to a stranger.



Odd ways to pay

“Pay with Apple or Steam gift cards.” · “Send it as Bitcoin.”

Gift cards, crypto, cash handed to a courier, or a bank transfer to a personal account. These are hard to trace and very hard to get back.

DO THIS No real company, council, HMRC or the police will ever ask you to pay with gift cards or crypto. If they do, it is a scam.



Still spotting...

6

The number looks right

The caller ID says your bank. The text sits in your bank's usual thread.

Criminals can fake (“spoof”) the number or name that shows on your phone, even your bank’s real number. A familiar name on screen proves nothing.

DO THIS Hang up and call back on a number you know. Use another phone, or wait a few minutes, as scammers can keep the line open. 159 can’t be faked.

7

Parcel, tax, toll and bank texts

“Missed delivery: pay £1.45 to rebook.” · “HMRC: you’re due a tax refund.”

Fake texts and emails about parcels, refunds, unpaid fines, tolls, parking or a “blocked” bank card. The link goes to a copycat site that steals your card details.

DO THIS Don’t tap the link. Forward scam texts free to 7726. Go to the real website by typing its address yourself. HMRC never tells you about a refund by text.



Romance that asks for money

“I wish I could meet you, but I need help with the flight.”

Someone you met online or in a game is loving and attentive but can never meet or video call. Then comes an emergency, a fee, or a “great investment”. UK Finance reported £39.2 million lost to romance scams in 2025, up 23%.

DO THIS Never send money to someone you haven’t met in person. Talk it over with a friend or family member you trust.



Investment “opportunities”

“Guaranteed 20% a month.” · A celebrity “backs” this crypto app.

Fake adverts on social media, deepfake celebrity videos, and friendly “account managers” on WhatsApp or Telegram. In 2025 investment scams caused the biggest losses of any bank-transfer scam type: £221.5 million, up 40% (UK Finance).

DO THIS Never invest after a cold call or advert. Check the firm on the FCA Register and Warning List at [fca.org.uk](https://www.fca.org.uk) before you pay a penny.



“Hi Mum, it’s me”

*“Hi Mum, I dropped my phone, this is my new number.
Can you pay a bill for me?”*

A message from a “new number” claiming to be your child, grandchild or friend, then an urgent request for money. AI can now copy a voice from a short clip.

DO THIS Call them on their old number or ask a question only they would know. Agree a family password for emergencies.

Spotted one? Stop, check, protect. Stop before you click, pay or share. Check it yourself using details you already trust. If money or your bank details are involved, call your bank straight away.



Your bank will never...

Your bank, the police or HMRC will NEVER:

- ask for your **PIN** or your **full online banking password**, not even by tapping it into your phone keypad
- ask you to read out or forward a **one-time passcode** sent to your phone
- ask you to move money to a “**safe account**”, even one they say is in your name
- send a **courier or taxi** to collect your cash, cards, PIN or cheque book
- ask you to **withdraw cash** or **buy gold, watches or gift cards** for “safekeeping” or to help an investigation
- rush you or tell you to **keep it secret** from your family or the bank staff

If anyone asks for any of these, it's a scam, however real they sound and whatever number shows on your phone.

GOT A CALL “FROM YOUR BANK”? DO THIS

1. Stop

Don't give any details, press any buttons or move any money.

2. Hang up

End the call. A real bank won't mind. Use another phone or wait a few minutes, in case the line is still open.

3. Call 159

It connects you safely to your own bank. It's run by Stop Scams UK, covers more than 99% of UK current accounts, and can't be spoofed.

QUICK CHECKS BEFORE YOU PAY OR SHARE

- Did they contact **me**, out of the blue?
- Am I being rushed, scared or flattered?
- Am I being asked for a code, PIN or password, or to move money?
- Do they want gift cards, crypto, cash or a bank transfer to a person?
- Can I check this myself, using a number or website I found, not one they gave me?

One “yes” to any of the first four is enough to stop. It’s always OK to say no, hang up or ignore it. Only criminals get angry when you check.



ACT FAST, DON'T PANIC

If it's happened to you

It isn't your fault, and you are not alone. The sooner you act, the better the chance of stopping payments and getting money back.

In Scotland: what to do, in this order

1

Call your bank now. Use the number on the back of your card, or call **159**. Tell them it's a scam. They can freeze cards and accounts, try to stop payments and start a refund claim. Call any other bank or card company involved too.

2

Report it to Police Scotland on 101. It's free, 24 hours a day. Call **999** if a crime is happening now or you are in danger. Write down your crime reference number.

3

Report the message. Forward scam texts free to **7726** (it spells SPAM). Forward scam emails to report@phishing.gov.uk. Fake HMRC texts go to 60599 and emails to phishing@hmrc.gov.uk.

4

Get advice: Advice Direct

Scotland. Free on **0808 164 6000**

(Mon to Fri, 9am to 5pm) or
consumeradvice.scot. They pass details to
Trading Standards.

5

Look after yourself. Stop all contact
with the scammer and keep screenshots as
evidence. Talk to someone. Victim Support
Scotland's free helpline is **0800 160
1985**.

Living elsewhere in the UK? Action Fraud has been replaced by **Report Fraud** (since 4 December 2025):
reportfraud.police.uk or 0300 123 2040. It covers England,
Wales and Northern Ireland only. It asks people in
Scotland to call Police Scotland on 101 instead. Many
leaflets and websites still say "Action Fraud". In Scotland,
read that as "call 101".

Beware the second scam. After a scam, criminals often
call back pretending to be the police, your bank or a
"recovery" firm that can get your money back for a fee.
Hang up. Your bank, the police and the free services on
this page never charge to help.



WANT THE WHOLE STORY?

Money: From Shells to Scams

This mini guide is a taster. The full guide goes much deeper: how scams work, the twenty main types doing the rounds in the UK, and exactly what to do to protect yourself and get your money back.

The story of money

From shells and coins to banknotes, cards and crypto, and the scams that grew up alongside each one.

The scammer's playbook

The four pressure levers every scam uses, and a full red-flag checklist.

20 scam types, explained

Phishing, safe-account calls, romance, investment, recovery, marketplace, tickets, car buying, rogue traders, pensions, AI voice cloning, QR codes, sextortion and more.

New in 2025–26

Fake fines, tolls and parking, cost-of-living and benefit scams, and four real-looking fakes, annotated.

Cybercrime made simple

Account takeover, SIM swaps, data breaches, two-step login and passkeys.

Where scams are heading

Deepfake calls, AI assistants, digital ID and the digital pound.

Protect and recover

The first-hour timeline, getting your money back, and a family scam plan.

Test yourself

A spot-the-scam quiz, scam myths checked, and a quick-reference card for the fridge.

Money: From Shells to Scams

£3.99

Full guide: 73-page A4 edition plus a phone edition ·

Written for Scotland, useful across the UK

clarityhq.uk/guides/avoiding-scams.html

Free guides on money, food, health, Fife and more:

clarityhq.uk

Type the address into your browser.

Please share this mini guide. Print it, forward it, pin it up at work, or send it to someone who might need it.

*In a world full of disinformation, get **Clarity**. · Made in Fife*

Published by Clarity Guides, Fife, Scotland. For general information only, not legal or financial advice. Phone numbers, figures and services were checked against official sources (Police Scotland, Report Fraud, GOV.UK, HMRC, Ofcom, Stop Scams UK, UK Finance, the FCA, Advice Direct Scotland and Victim Support Scotland) on 22 October 2026. Services can change, so if in doubt, check the official website by typing its address yourself. Loss figures are from UK Finance's Annual Fraud Report 2026, covering 2025. Cover and illustrations drawn in code. No AI images.