FREE CHEAT SHEET

The 10 Scam Red Flags

Spot almost any scam in 10 seconds — a free guide from *The Scam Protection Blueprint* by a cybersecurity professional.

Today's scams are built to look real and to make you **panic** — they sound like your bank, or a message from your own child. But almost every one trips at least one of these ten wires. Learn to spot them, print this out, and keep it where you'll see it. The moment you notice a flag, you stop, and the scam falls apart.

1 Urgency & pressure

"Act now or your account closes." Real organisations give you time. Manufactured panic is the scammer's #1 tool.

2 Out-of-the-blue contact

A call, text or email you didn't start, about money, an account or a "problem." Treat every one as suspect until proven otherwise.

3 "Move your money to keep it safe"

No bank, police force or agency will *ever* tell you to transfer money to a "safe account." This one is always a scam.

4 They want a code, PIN or password

Nobody legitimate needs your one-time code, PIN or password. Anyone who asks is trying to get in, not help you.

5 Odd payment methods

Gift cards, crypto, vouchers, or a transfer to a brand-new account. Real bills are never paid in gift cards.

6 "It's me — I'm in trouble"

A child or friend messaging from a *new* number needing money fast. Always verify on the number you already have.

7 Too good to be true

Guaranteed returns, a prize you didn't enter, a refund you're owed. If it's free money, it's bait.

8 Almost-right details

A lookalike email address, a slightly-off web link, a fuzzy logo, or "Dear Customer" instead of your name.

9 "Don't hang up. Don't tell anyone."

Keeping you on the phone and discouraging you from checking is a giant tell. Honest callers are happy for you to verify.

10 "Install this / share your screen"

Remote-access apps hand a stranger your device. Never install software because someone on the phone told you to.

The one rule that beats every scam

MEMORISE THIS

Stop. Don't act. Verify it yourself. Hang up the phone or close the message, then contact the bank, company or person using a number or website **you** look up — never the one they gave you. A genuine request survives a pause; a scam does not. When in doubt, the answer is always to slow down and check.

Set a family "safe word"

Agree one word that only your family knows. If a panicked "emergency" call or text ever asks for money, ask for the word. A real loved one can say it — a scammer (or an AI voice clone of them) cannot. It's the simplest defence against the fastest-growing scam of 2026.

Do these three things this week

- Turn on two-step verification for your email and banking apps.
- Agree the safe word above with the people you love.
- Tell one older relative about red flags #3 and #9 — the two that cost people the most.

If it's already happening — get free help fast

- UNITED KINGDOM
  Call **159** to reach your bank safely · Action Fraud **0300 123 2040**
- UNITED STATES
  Report at **reportfraud.ftc.gov** · **identitytheft.gov**
- CANADA
  Anti-Fraud Centre **1-888-495-8501** · antifraudcentre.ca
- AUSTRALIA
  scamwatch.gov.au · IDCARE **1800 595 160**