Don't Get Scammed

A Plain-English Guide to Online Fraud

Written for people who think they'd never fall for it — because that's exactly who scammers target.

It can happen to anyone

Scammers don't just target the naive. They target the busy, the trusting, the polite, and the stressed. Doctors, lawyers, engineers, retired professionals — all have been conned. In 2025, UK fraud losses exceeded £1.5 billion. The average victim loses over £2,000 before they realise what's happened.

The reason clever people get caught is that modern scams are designed by professionals using psychology, not just technology. They exploit fear, urgency, authority, and isolation — the same techniques used by hostage negotiators and cult leaders. Understanding how they work is the best protection you have.

Part 1: The psychology — how scammers manipulate you

Before looking at specific scams, understand the five techniques every scam uses. Once you recognise these, you'll spot scams instinctively.

1. Urgency — "Act now or else"

Every scam creates a time pressure. "Your account will be closed in 24 hours." "This offer expires today." "Respond immediately to avoid prosecution." The purpose is to stop you thinking clearly. A calm person asks questions. A panicked person clicks links.

> **The defence: If someone is pressuring you to act immediately, that pressure IS the scam. No legitimate organisation will punish you for taking 24 hours to verify something.**

2. Authority — "This is HMRC / your bank / the police"

Scammers impersonate organisations you trust and fear. A call from "HMRC" saying you owe unpaid tax. An email from "your bank" about suspicious activity. A text from "Royal Mail" about a delivery.

Critically, scammers can now display your bank's real phone number on your screen. It's called "caller ID spoofing" — they use internet phone services that let them set any number as the outgoing display. It costs pennies. Your phone shows "Barclays 0345 734 5345" but the caller is a criminal in a call centre anywhere in the world.

Even worse: on a landline, the scammer can hold the line open after you hang up. You pick up the phone, dial your bank, and you're still connected to the scammer — who plays a fake dial tone. This can last up to 2 minutes.

> **The defence: Hang up. Wait 5 minutes. Use a different phone (your mobile, not your landline) and call your bank on the number on the back of your card. Or dial 159 — the national Stop Scams UK number that connects you directly to your real bank's fraud team.**

3. Fear — "Something terrible will happen"

"Your account has been compromised." "A warrant has been issued for your arrest." "Your grandchild has been in an accident." Fear bypasses rational thought. When you're frightened, you stop asking "is this real?" and start asking "how do I make this stop?"

> **The defence: Take a breath. Real emergencies come through real channels — the police come to your door, hospitals call from known numbers, banks send letters. Nobody who genuinely needs to help you will object to you verifying their identity first.**

4. Isolation — "Don't tell anyone about this"

Scammers always discourage you from talking to family, friends, or the actual organisation being impersonated. "This is a confidential investigation." "Don't discuss this with anyone or the criminals will be alerted." The moment someone tells you not to talk to anyone else, they're trying to stop someone else from recognising the scam.

> **The defence: Tell someone. Always. Before you do anything, tell a family member, a friend, or a neighbour. Scammers cannot survive scrutiny from a third party.**

5. Reciprocity — "I've helped you, now help me"

Some scams start by doing you a favour. A "tech support" agent fixes a problem on your computer (that they created). A friendly stranger online gives you investment advice that works (with small amounts, to build trust before the big ask). We are wired to repay kindness. Scammers exploit this.

> **The defence: If someone you've never met is being unusually helpful or generous, ask yourself what they're getting out of it.**

Part 2: The scams — what's out there

Phishing emails — "Your account needs attention"

You receive an email that looks like it's from your bank, Amazon, PayPal, HMRC, or Netflix. The logo is correct, the language is professional, and the email address looks almost right. It asks you to "verify your account" or "update your payment details." The link takes you to a fake website. You enter your login details. They now have your password.

> *Example: "Dear Customer, We have detected unusual activity on your Barclays account. For your security, please verify your identity within 24 hours or your account will be temporarily suspended." The sender reads barclays.security@mail-verify.com — not barclays.co.uk.*

Be aware that scammers can fake the "From" field — an email can display "security@barclays.co.uk" even when sent from a criminal's server. One useful technique: hit "Forward" instead of "Reply" to reveal the true sender address. But even this isn't foolproof. The only safe rule: never click a link in any email from a bank. Open a new browser tab and type the address yourself. Every time. No exceptions.

Smishing — scam texts

You receive a text from "Royal Mail," "HMRC," or a "delivery company." It says a parcel couldn't be delivered and you need to pay a small redelivery fee. The link captures your card details. The small amount — usually £1.50 to £3.00 — is designed to seem too trivial to worry about. But the real purpose is capturing your card number.

> *Example: "ROYAL MAIL: Your parcel could not be delivered. A redelivery fee of £1.45 is required. Pay here: royalmail-redelivery.com" — the real site is royalmail.com.*

Vishing — phone scams

Someone calls claiming to be from your bank's fraud department. They say your account has been compromised and you need to transfer money to a "safe account." They may know your name, address, and last few digits of your account number (from data breaches). The "safe account" is the scammer's account.

> **Banks will NEVER ask you to transfer money to a "safe account." Hang up, wait 5 minutes, and call 159 — the national Stop Scams UK helpline. Never use the same landline you received the call on.**

Romance scams — "I think I'm falling for you"

Someone contacts you on a dating site or Facebook. They're attractive, attentive, and say all the right things. Over weeks or months, they build a genuine-feeling relationship. They never video-call. Eventually, they need money — a medical emergency, a flight to come and see you. You send money. They disappear, or ask for more.

> **If someone you've never met in person asks for money — for any reason — it's a scam. No exceptions. Reverse-image-search their profile photo — stolen photos are the number one tool.**

Investment scams — "Guaranteed returns"

You see an advert — often with fake celebrity endorsements — for cryptocurrency or property investment promising exceptional returns. You invest £250. A dashboard shows your money growing. You invest more. When you try to withdraw, there are fees, delays, excuses. Your money is gone. Everything on the screen was fake.

No legitimate investment guarantees returns. Check the FCA register (register.fca.org.uk) before investing with any company.

Tech support scams — "Your computer has a virus"

Someone calls from "Microsoft" or a pop-up appears saying "Your computer is infected — call this number." They ask you to install remote access software. Once they have access, they can see your files, passwords, and bank login.

Microsoft, BT, and Apple will never call you about a virus. If a pop-up locks your browser, press Ctrl+Alt+Delete to close it.

Courier fraud — "The police need your help"

Someone calls claiming to be a police detective investigating fraud at your bank. They ask you to withdraw cash and hand it to a "courier" as evidence. The courier is the scammer.

Police will NEVER ask you to withdraw cash, buy gift cards, or hand over money. Never. Call 101 to report it.

Grandparent scams — "It's me, I'm in trouble"

You receive a call from someone claiming to be your grandchild. "I've been in an accident / arrested. Please don't tell Mum and Dad — just send money." With AI voice cloning, scammers can now replicate a person's voice from a few seconds of social media audio.

If a family member calls in distress asking for money, hang up and call them back on their normal number. A familiar voice is no longer proof of identity.

Impersonation — fake emails from people you know

You receive an email from your boss asking you to buy gift cards or make a bank transfer. The email address is slightly different. Any request for gift cards is a scam — no legitimate business transaction involves gift cards.

Part 3: What to do if you've been scammed

Don't be embarrassed. Report it. Scammers are professionals — feeling ashamed is what stops people reporting, which is exactly what scammers want.

Immediate steps

★ Contact your bank immediately. Call 159 (Stop Scams UK) or your bank's fraud line. They may be able to freeze or reverse the transaction.

★ Change your passwords if you've entered login details on a fake website — and any other accounts using the same password.

★ Report it to Action Fraud: 0300 123 2040 or actionfraud.police.uk

★ Report scam texts by forwarding to 7726

★ Report scam emails by forwarding to report@phishing.gov.uk

★ Tell someone. A family member, a friend, a neighbour.

Long-term protection

★ Never click links in unexpected emails or texts — go to the website directly.

★ Use different passwords for different accounts. A password manager like Bitwarden (free) makes this easy.

★ Enable two-factor authentication on your email, bank, and social media.

★ Keep your phone and computer updated — security updates fix vulnerabilities.

★ Be sceptical by default. If something feels wrong, it probably is.

The golden rules

1. If in doubt, do nothing for 24 hours. No legitimate situation will be harmed by a pause. Every scam will be defeated by one.

2. Dial 159 if you're unsure. The national Stop Scams UK number connects you to your real bank.

3. No legitimate organisation will pressure you to act immediately.

4. No bank will ask you to transfer money to a "safe account."

5. No police officer will ask you to withdraw cash.

6. No government agency will demand payment by gift card or cryptocurrency.

7. Anyone who tells you not to talk to family or friends is trying to scam you.

8. Never click a link in an email from a bank — type the address yourself.

9. If it sounds too good to be true, it is.

The bottom line

Scammers are not amateurs sending badly-spelled emails from Nigeria. They are organised, well-funded criminal operations using AI, stolen data, psychological manipulation, and professional-quality websites. They run call centres. They have scripts. They practice.

The best defence isn't technology — it's a pause. Before you click, before you call back, before you transfer, before you share — pause. Talk to someone. Check the real website. Call the real number. That five-minute pause is worth more than any antivirus software on the market.

Sources

1. UK fraud losses 2025 — UK Finance Annual Fraud Report 2025
2. Action Fraud reporting — actionfraud.police.uk
3. FCA register — register.fca.org.uk
4. Report scam texts to 7726 — Ofcom guidance
5. Report phishing emails — NCSC, report@phishing.gov.uk
6. AI voice cloning in scams — Which? investigation, 2025
7. Romance scam statistics — National Fraud Intelligence Bureau, 2025
8. Celebrity endorsement scams — MoneySavingExpert warnings
9. Courier fraud warnings — City of London Police / Take Five campaign
10. Landline call not disconnecting — Ofcom consumer guidance
11. 159 Stop Scams UK helpline — stopscamsuk.org.uk
12. Caller ID spoofing — Ofcom guidance; Action Fraud alerts
13. Email header spoofing — NCSC guidance on email authentication

This guide was written for the community. Share it with anyone who might find it useful.