

Scams & Fraud

Recognising and avoiding common scams — for anyone new to online safety.

Why It Matters

Scams are everywhere — emails, texts, social media, even phone calls. They don't just target the careless; they target the kind, the busy, and the trusting. Learning how scammers work helps you spot the tricks before they cost you money or confidence.

How Scams Work

Scammers rely on three things: **speed, fear, and familiarity**. They make you act fast, worry you'll lose something, or pretend to be someone.

 **Message scams** | “Your parcel is waiting” — fake texts or emails.

 **Call scams** | “Your account's been locked” — someone pretending to be your bank.

 **Shopping scams** | Fake websites selling items that never arrive.

 **Romance scams** | Emotional manipulation that leads to requests for money.

 **Investment scams** | Unrealistic returns or crypto “opportunities.”

Stay Scam-Aware

-  **Pause before you act.** Pressure is a red flag.
 -  **Check the source.** Contact the company directly through official details.
 -  **Avoid clicking links** in unexpected messages.
 -  **Never share codes or passwords** with anyone — even “bank staff.”
 -  **Talk before you transfer.** Ask a friend or family member to sanity-check it first.
-

If You Think You've Been Scammed

- 1 Stop contact** with the scammer immediately.
- 2 Inform your bank** as soon as possible — they can try to recover funds.
- 3 Report it** at report@phishing.gov.uk or <https://www.actionfraud.police.uk/>
- 4 Get support.** It's okay to feel shaken — you're not alone.