

Is this a scam?

Scammers now use AI to write perfect messages and copy voices. So don't judge how real it looks or sounds. Judge what it's asking for.

The five red flags

- **Hurry.** "Act now." "Today only." "Your account will be closed."
- **Money or codes.** Asking you to pay, move money, or share a PIN, password or one-time code.
- **Secrecy.** "Don't tell anyone." "Don't tell the bank."
- **Odd ways to pay.** Gift cards, cryptocurrency, or a transfer to a "safe account".
- **Too good to be true.** Guaranteed returns, surprise prizes, amazing bargains.

Two or more together? Stop. Don't click, don't pay, don't reply.

What to do

1. **Stop.** A real bank, the police or HMRC will never rush you.
2. **Hang up.** Then call back on a number you already trust, such as the one on your bank card.
Most UK banks can also be reached safely by calling **159**.
3. **Never share** PINs, passwords or one-time codes. Your bank will never ask for them.

Our family code word

A word only your family knows. If someone calls saying they're a relative in trouble, even if it sounds just like them, ask for the word.

Our word is kept safe with: _____

Report it (UK)

Scam text	Forward it to 7726 (free)
Scam email	Forward it to report@phishing.gov.uk
Lost money?	Call your bank straight away, then report it at reportfraud.police.uk
Advice	Citizens Advice consumer helpline: 0808 223 1133

Free to print and share. More plain-English help: deadeasyai.com/learn