Stop and check

The short version: If a call, text or email you did not expect is about money, a crime, your accounts, a code or a gift card, stop. Hang up. Then check yourself, in a way you choose.

You do not have to decide if the caller is real. You follow three rules.

Rule 1: Hang up and call back

- Hang up, or stop replying. Do not tap a link in the message.
- Contact the company or agency yourself. Use a number from its real website, the back of your card or your bill.
- Never use a number the caller gave you. Never search for words the caller told you to search for.
- The name or number on your screen can be faked. This is called “spoofing.”
- You do not need a reason to hang up. You can say: “I’ll call the bank myself. Goodbye.”
- If the caller rushes you, gets angry or says you will be in trouble, that is a sign of a scam.

What real banks and police do not do. In the UK, genuine banks, police and service providers will never call to ask you to move money, share your financial details, or hand over remote control of your computer. In the US too, do not move money because an unexpected caller tells you to. Hang up and contact your bank yourself.

In the UK: after you hang up, criminals can sometimes keep a landline connected. Use a different phone to call back if you can. If you must use the same landline, wait at least 10 minutes first.

Rule 2: Never read out a code

- A code is the short number a website or app sends when you sign in. A sign-in code helps a service check that it is you. It may be used as an extra sign-in step.
- If someone who contacted you asks you to read out a code, it is a scam. This is true even if they say they are your bank, a tech company or a government agency.
- Do not tap “approve” on a sign-in request you did not start.
- This is also true for your PIN, your recovery codes and your password. Never give them to someone who calls or messages you.

Rule 3: Gift cards are for gifts

- No real company, bank, police force or government office asks you to pay with a gift card.
- If someone tells you to buy a gift card and give them the numbers on the back, it is a scam.
- Be careful, too, if you are pushed to pay by wire or bank transfer, crypto (digital money) or a payment app. These can be hard to undo.

Do this today

1. Save your bank’s number in your phone, copied from the back of your card.
2. Save your phone company’s number, copied from your bill.
3. Tell someone close to you: “If anyone calls about money, a code or gift cards, we hang up and call back ourselves.”

Checked: 8 Nov 2026