Scam telephone calls (Vishing)

Fraudsters may phone you and claim to be from a bank, police, or other reputable organisations, in an attempt to obtain your personal information and banking details. Fraudsters may even try to trick you into allowing them access to your computer to steal your money.

Regardless of how professional or convincing a caller sounds, remember a bank, police or other trusted organisations will **never** contact you by any means to:

- Ask for your financial information or your full security details.
- Ask you to provide your PIN code or requests to collect your bankcard from your home address.
- Ask you to provide a card reader code or token code.
- Ask you to move your money to a new or 'safe' account.

How to protect yourself from telephone scams

1. Always be wary of unexpected cold calls. Say no to requests for information and don't be afraid to terminate the call.
2. Never respond to callers who ask you to confirm your PIN, card reader codes or token codes, or to request to collect your bank card from your home address. Banks will never ask you to do this.
3. Never respond to a request to transfer your funds to another bank, even if the caller advises you that you need to urgently move your money to a 'safe' bank account. Banks will never ask you to do this.
4. Never respond to a caller who asks you to log on to online banking or a request that allows them remote access to your computer.
5. Don't assume a call is genuine because they know personal details about you or by the caller ID information. Fraudsters can copy the telephone number of an organisation and make it appear on the caller ID display.
6. If you want to validate a phone call use contact details obtained from a reliable source.

→ **Always stop and think – is this a genuine call?**

Take Five to stop fraud

Received a phone call, text or email asking for your personal or financial information? If so, what do you do? Before you act, stop. Take a moment to assess the situation. The information below should help you work out whether that request is legitimate.

1. Never give out your security details (such as your PIN or full banking password)

A genuine bank or organisation will never ask you for these in an email, on the phone or in writing. Consider what you're being asked for. Question why they need it. If you aren't 100% sure who you're talking to, don't give them your personal or financial details.

2. Don't assume an email, text or phone call is authentic

Even if someone seems to know your basic details, it doesn't mean they're genuine. In an attempt to gain your trust, fraudsters may claim you've been a victim of fraud. They often do this to get you talking, then try and persuade you into giving them your security details.

3. Don't be rushed, or pressured, into making a decision

No genuine bank or trusted organisation will, under any circumstances, force you to make a financial transaction on the spot. Neither would they ask you to transfer money into another account for reasons relating to fraud. If you're asked to do this, then stop and consider what they are asking you.

4. Listen to your instincts

Does a situation feel wrong or strange? If so, it's usually right to question it. Fraudsters will try to manipulate you: they'll try and lull you into a false sense of security when out and about, or rely on your defences being down when you're at home. They'll try to appear trustworthy, but they may not be what they appear.

5. Stay in control

Be confident. It's always okay to stop a conversation. You can always refuse unusual requests for personal or financial information.