

Scams & online safety | Easy | 2 min read

How to spot a scam email, text or call

Scammers pretend to be banks, delivery firms, the tax office or people you know. Their messages are designed to rush you. The best defence is to slow down and check through a route you trust.

Common warning signs

- The message is unexpected, or says you must act now, or something bad will happen.
- It asks for personal details, passwords, PINs, codes or payment.
- It comes from a strange address or number, or the wording and spelling are odd.
- It offers a prize, refund or too-good-to-be-true deal.
- A caller says they are from your bank, the police or tech support and asks you to move money or let them onto your computer.

What to do

1. Stop. Do not click links, open attachments, reply or call back on a number in the message.
2. Check independently. Contact the organisation through its official app, website typed in yourself, or the number on your card or bill.
3. Hang up if a call feels wrong. Wait a few minutes, then call back on a number you know to be real, ideally from a different phone.
4. Never share one-time codes or passwords with anyone. Real firms will not ask for them.
5. Never let a stranger take remote control of your computer.

Report it

- Forward scam texts to 7726 (free).
- Forward scam emails to report@phishing.gov.uk.
- Report fraud and cyber crime to Report Fraud (formerly Action Fraud) at reportfraud.police.uk or on 0300 123 2040. In Scotland, call Police Scotland on 101.

When to get more help

If you have already clicked, paid or shared details, do not panic. Phone your bank straight away using the number on your card, and ask for help changing passwords. Stop and ask for help if you gave someone access to your computer or are being pressured right now. Tell us what happened and keep the message.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.