Cyber Protect

Always Take Five to Stop Fraud

Phone Calls

Phone numbers can be spoofed so that scammers appear to be ringing you from a business, service or organisation you trust.

Never respond to an unexpected caller or give them computer access.

Emails & Messages

Emails can be spoofed so the sender's address you see appears to be that of someone you know or trust.

Never click links in unexpected emails. Verify them using a separate trusted phone number.

Text Messages

Text messages can be spoofed so they appear to come from trusted friends, colleagues and services.

Never click links in text messages or make any requested payments unless you've verified the source.

Social Media

Social media accounts and content can be made to look like your bank's real customer helpline and info.

Never reveal passwords, PINs, personal information or bank details unless you have verified the account.

Alerts & Warnings

Computer or phone alerts may tell you to contact fake IT helplines, install software or pay for a subscription.

Never contact or pay these scammers. Instead seek advice from a friend or reputable IT company.

takefive-stopfraud.org.uk