Phone scams
Fraud over the phone – or vishing – is when a fraudster calls claiming they're from your bank or another trusted organisation, often under the pretence there has been fraud on your account. It is easy for them to convince you too, since they can both fake the telephone number on the screen and do their research to find out some of your basic bank and personal details. Remember though, a genuine bank will never ask you for personal financial details like your PIN number or full banking password (even by tapping it into your phone keypad), or ask you to transfer money directly to them.

Text message scams
A text might not be from who you think it is – Smishing is when fraudsters pretend a message is from your bank or another organisation you trust. They will usually tell you there has been fraud on your account and will ask you to deal with it by calling a number they provide or by visiting a fake website to update your personal details. Please take a moment to stop and think and realise this is the fraud, and any data you enter will be captured by them.

Online fraud
Online fraud covers everything from online shopping to online banking, but one thing can help prevent both: take the time to install security software and updates most banks and browsers offer. These can help protect you whether the fraudsters are trying to dupe you with fake pop-ups in your online banking window, sending you 'scam alert' messages that hide malware, or faking retailer websites to make you input your financial details.

Email scams
Fraudsters don't just try to contact you by phone and text, they also 'phish', contacting you by email, usually saying you need to verify or update some details or reactivate an account. So always be suspicious of unsolicited emails that are supposedly from your bank or some other trusted organisation because the address can easily be faked. Never automatically click on any links they contain either, not before stopping to check if they seem genuine first.

What to do if you think you're a victim
If you think there has been fraud on your card or bank account – or if you suspect someone has attempted to compromise your financial details – report it immediately to your bank or other financial services provider and then contact Action Fraud on 0300 123 2040 or at **actionfraud.police.uk.**

Take Five is a national campaign that offers straightforward and impartial advice to help everyone protect themselves from preventable financial fraud. This includes email deception and phone-based scams as well as online fraud – particularly where criminals impersonate trusted organisations. Led by Financial Fraud Action UK Ltd (FFA UK), it is being delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector. Visit: takefive-stopfraud.org.uk for more information about Take Five and which partners are involved.

takefive-stopfraud.org.uk

IT PAYS TO TAKE TIME TAKE FIVE TO STOP AND THINK

TAKE FIVE

TO STOP FRAUD™

If you receive a phone call, text or email asking you to hand over personal or financial information, you need to take a moment to reflect and step back from the situation.

Yes, even if they say they're the bank, police or another trusted organisation, you still need to take the time to stop and think about what's really going on.

Because, deep down, you probably already know the basic rules on how to beat financial fraud – you just need to take a deep breath and stay calm to remember them...

General advice

1

Never disclose security details, such as your PIN or full banking password
Banks and other trusted organisations will never ask you for these in an email, on the phone, by text or in writing. Before you share anything with anyone, stop. Then pause to consider what you're being asked for and question why they need it. Unless you're 100% sure who you're talking to, don't disclose any personal or financial details.

2

Don't assume an email or phone call is authentic
Just because someone knows your basic details (such as your name and address or even your mother's maiden name), it doesn't mean they are genuine. Be mindful of who you trust – fraudsters may try to trick you and gain your confidence by telling you that you've been a victim of fraud. Fraudsters often use this tactic to draw you into the conversation, to scare you into acting and revealing security details. Remember, fraudsters can also make any telephone number appear on your phone handset, so even if you recognise the number or it seems authentic, do not assume they are genuine.

3

Don't be rushed or pressured into making a decision
Under no circumstances would a bank or organisation force you to make a financial transaction on the spot; they would never ask you to transfer money into another account for fraud reasons. Remember to stop and take time to carefully consider your actions. A bank or trusted organisation won't rush you or mind waiting if you want time to think.

4

Listen to your instincts
If something feels wrong then it is usually right to question it. Fraudsters may lull you into a false sense of security when you are out and about or rely on your defences being down when you're in the comfort of your own home. They may appear trustworthy, but they may not be who they claim to be.

5

Stay in control
Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel embarrassed when faced with unexpected or complex conversations. But it's okay to stop the discussion if you do not feel in control of it.