Helping you to stay safe

Tips to reduce the threat of fraud and scams

- **Protect your personal and security details**
  A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or security numbers. Don't give out personal or financial details unless it's to use a service that you have signed up to, and you're sure that the request for your information is directly related.

- **Never set up new or change existing payment details, without first verifying the request directly with the person or company you're paying**, preferably using existing contact details.

- **Never transfer money out of your account if asked to do so for 'security reasons'**
  If you're asked to transfer money out of your account for security reasons, end the call immediately, ensuring the previous caller has disconnected and call us.

- **Never reply to emails asking for your personal or 'security information'**
  We'll never email you to ask for your information. If you get an email like this, it could be a fraudster trying to get your confidential information. Our emails will always be addressed to you and won't have a standard 'Dear Customer' greeting.

- **Download free online security software**
  We recommend that you use the trusted online security software Trusteer Rapport. This is free and it helps to protect you when using Online Banking. It can also be used alongside any standard anti-virus product.

Our top three tips

1. **Never** share a Santander One Time Passcode (OTP) with another person. Not even a Santander employee.
2. **Never** download software or let anyone log on to your computer or devices remotely during or after a cold call.
3. **Never** enter your Online Banking details after clicking on a link in an email or text message.

We care

If you think you've been a victim of a fraud or scam, or are concerned that your personal or security details may have been compromised, please call us immediately on **0800 9 123 123.**

For more information on how to protect yourself from fraud and scams visit our website: **santander.co.uk**

STOP
Taking a moment to stop and think before parting with your money or information could keep you safe.

CHALLENGE
Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT
Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

Santander has joined other banks and companies in Take Five, an initiative led by Financial Fraud Action UK. Its aim is to encourage people to think about fraud, with five steps in mind. Take a look at the Take Five website to learn more www.takefive-stopfraud.org.uk

MISC 2349 MAY 20 H

This item can be recycled.

Santander

How to protect yourself against scams

- Understand how the most common scams work
- Protect yourself from becoming a victim

Common scams – how to stay safe

Selling scams

A buyer of something that you're selling could be a potential fraudster.

The buyer pays more than the value of the item being sold. They ask for the extra money to be transferred back or sent to a third party, for example a 'shipping agent'. The buyer disappears, leaving you out of pocket.

Smishing

Fraudsters send spoofed texts that appear to be from your bank or another trusted organisation with a sense of urgency to contact them.

The text may even fall into previous genuine text threads, making it look legitimate.

Never click on links sent in a text message, it may lead to a counterfeit website. Santander, or any trusted organisation, will NEVER ask you to move your money.

Payment redirection scam

Fraudsters may intercept or spoof an email between you and a legitimate contact, asking for payment for goods or services.

The fraudster may say that the bank account details for an outstanding or future payment need to be changed. The email will appear to be from your genuine contact.

Always verify payment details with the organisation or person directly on a trusted or public number, never respond using the contact details they have provided.

Friendship and romance scams

These scams happen when someone you've met online aren't who they say they are. Once they gain your trust, they ask for money for a variety of emotive reasons.

- Never send money to anyone you don't know and trust.
- Never reveal your security details such as your passwords or card details to someone you've met online.
- Only chat through the dating site where you met, not via your personal email or text.
- Protect your privacy and don't reveal too much information online, especially on social networks.

Telephone scams

Requests to move or withdraw your money

Criminals make contact posing as your bank or another organisation. The number they are calling from is fake to look the same as the genuine number. They may say:

- your account is at risk and you urgently need to move your money to a safe account
- you need you to withdraw cash to aid us with an investigation.

They might ask you to lie about the real reason for the transaction to avoid suspicion from the bank.

The account number you move your money to or the courier you hand the cash over to is in fact controlled by the fraudster.

Remote access scam

A fraudster contacts you saying they're from some kind of service provider, like telecommunications or an IT service, and will try to access your device.

They may offer to fix, upgrade or protect your devices. They may ask you to log onto your online banking and to download an app or software that allows them onto your device to 'help' you fix any problems.

Allowing them on like this, will allow them to access your personal and security data and possibly to make payments from your online banking.

Never allow anyone remote access or to connect to your devices following a cold call, text or email.

Other scams to be aware of

Buying scams

You find an item online, but after talking to the seller, you're told that the item (such as a car) can't be seen in person.

The seller persuades you to transfer money to secure the item. They may even send you a fake website link to make the payment.

Beware – the site may look like a well-known website, but the link will take you to a fake version of the site.

Once the funds are transferred into the fraudster's account, the seller and listing vanish, leaving you without the item or your money.

If buying from a reputable buying site, stick to the advice and process they've provided. Never communicate outside the site.