Staying safe

Key tips to help stop 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'**
  We'll never ask you to do this. If you're asked to transfer money out of your account for security reasons, end the call immediately 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.

Don't forget our top three tips

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

Contact information

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/securitycentre**

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 JAN '18 H

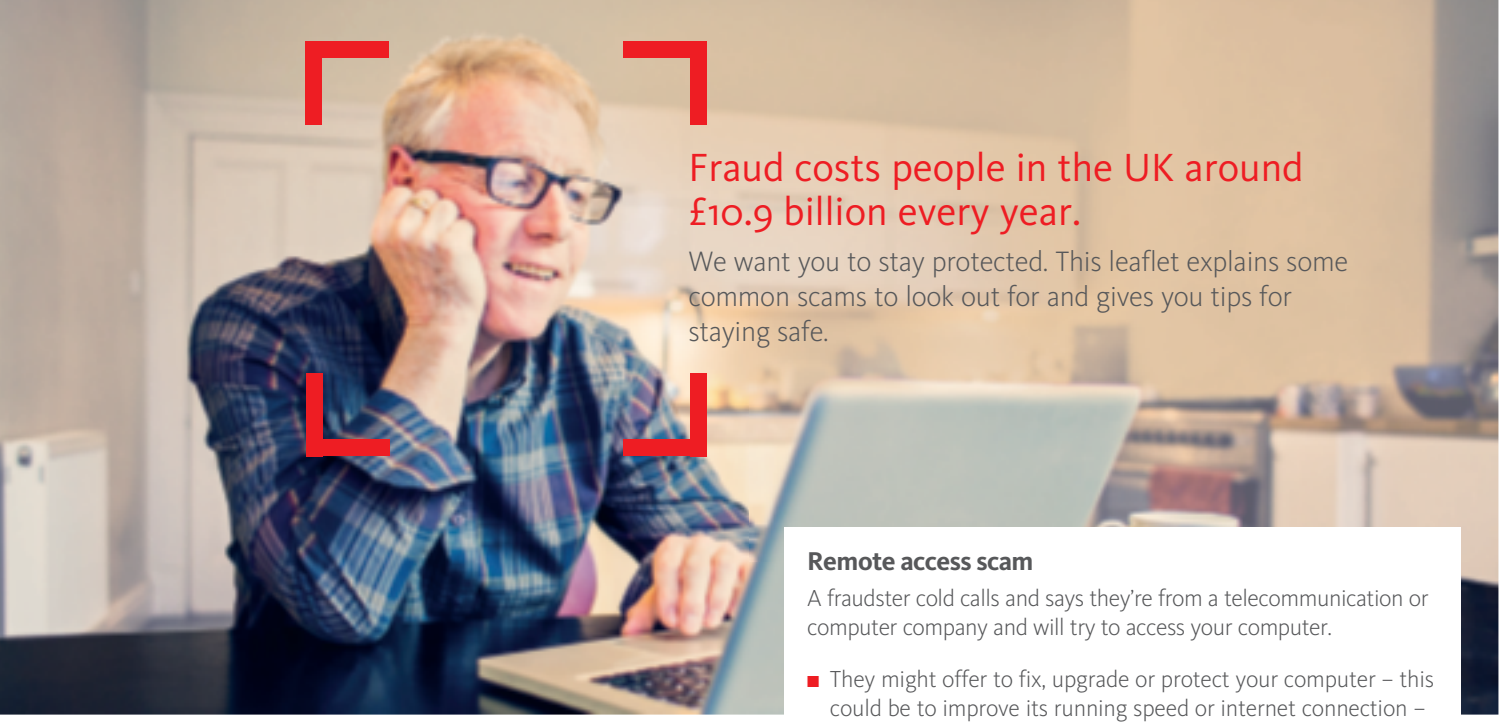
This item can be recycled.

How to protect yourself against scams

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

Here to help you prosper

Santander



Fraud costs people in the UK around £10.9 billion every year.

We want you to stay protected. This leaflet explains some common scams to look out for and gives you tips for staying safe.

Telephone scams

Requests to transfer funds

- This involves a fraudster calling you and posing as your bank or another organisation. The number they're calling from may be 'spoofed' to make it look like it's from your bank or another legitimate organisation.
- They tell you that you're at risk of fraudulent activity and must transfer your funds into a 'safe account'.
- You will often be pressured to act immediately.
- This 'safe account' is actually the fraudster's account, so your money is sent directly to the fraudster.

Requests to withdraw cash

Some fraudsters pose as police officers to persuade you to visit your local branch and withdraw funds from your account. They'll tell you that you're helping with a police investigation.

- The fraudster will tell you not to inform the staff at the branch of the real reason for the withdrawal.
- Once withdrawn, the money is collected in person from you by a courier or the fraudster themselves.
- Some fraudsters might ask you to make a high value purchase, for example a watch, which is collected by the fraudster.

Remote access scam

A fraudster cold calls and says they're from a telecommunication or computer company and will try to access your computer.

- They might offer to fix, upgrade or protect your computer – this could be to improve its running speed or internet connection – or for assistance for refunds of overpayments.
- These callers may ask you to log on to your online banking and will attempt to remotely access the computer to 'help' you with the problem.
- However, the remote access allows them to release malicious software and gain access to personal and security data. They may even be able to access your online banking directly.
- Never allow anyone remote access or connect to your computer following a cold call.

Other scams to be aware of

Buying scams

These scams are where you find an item online at a very reasonable price, but after talking to or emailing the seller, you're told that the item (such as a car) can't be seen in person.

- The seller will persuade you to transfer money to secure the item.
- Sometimes they send you a fake website link to send the payment. This is to make the transaction look real.
- Beware – the site may look like a well-known website, but the link will take you to a fake version of it.
- Once the funds are transferred into the fraudster's account, the seller and listing vanish. It'll leave you without the item or your money.

Selling scams

Be careful when you're selling something. A buyer could be a potential fraudster. Here's how they do it.

- The buyer will give you a cheque of greater value 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'.
- Once you have sent the extra money to the buyer, the cheque bounces and the buyer then disappears, leaving the you out of pocket.

Smishing

Fraudsters send texts saying that they're from your bank, and that they need you to update your personal details or speak with you urgently.

- The text message can fall into previous genuine text threads, this helps to make it look legitimate.
- The message normally contains a telephone number (premium rate) to call or a link to a counterfeit website that asks you to enter personal details or transfer money as your account is at risk.
- A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account.

Payment redirection scam

These scams happen when fraudsters intercept an email conversation between you and a legitimate contact who may be asking for payment for goods or services, like solicitors for a house purchase or a builder.

- The fraudster may say that the bank account details for an outstanding or future payment need to be changed and the email will appear to be from your genuine contact.
- Always confirm any change of payment requests with the company directly.
- Do not respond to the email address the request has been sent from or use the contact details they provided – use a previously used number to verify the change.

Friendship and romance scams

Dating or romance scams are when you think you've met your perfect partner online, but they aren't who they say they are. Once they've gained your trust, they ask for money for a variety of emotive reasons.

- Never send money to anyone you don't know and trust.
- Never give your credit card or online account details to anyone.
- Always chat through the dating site or chat room where you met – not via email.
- Protect your privacy and don't reveal too much information online, especially on social networks.