Santander

Fraud awareness

Knowledge is key in protecting yourself

Help keep yourself safe from fraud

We take security very seriously and want you to feel safe and secure banking with us. As well as the measures we have in place to protect you, there are a few things that you can do to help keep your details safe and secure. Understanding how to use your information in the correct way will help stop fraudsters getting hold of your personal and security details or tricking you into taking action on your account.

Please always keep our top tips in mind:

- **Never share a Santander One Time Passcode (OTP) with another person. Not even a Santander employee.**

  OTPs are used to verify online transactions or payments and are entered into your computer or mobile app to complete a transaction. You'll **never** need to give out an OTP, verbally or otherwise, to anyone for any reason and requests to do this will **always be fraudulent.**

- **Never download software or let anyone remotely log on to your computer or other devices, either during or after a cold call.**

  Be aware of callers who claim to be able to help with computer or internet related issues and who ask you to follow instructions to help resolve the issue. Fraudsters will try and access your computer or device to then gain access to your Online Banking and your money.

- **Never enter your Online Banking details after clicking on a link in an email or text message.**

  The text or email may appear to come from Santander but the links will send you to a fake website where the details you enter will be captured by a fraudster. We'll never send you a link telling you to log on to your Online Banking for any reason. If you need to log onto your account, you should always enter our full web address, **santander.co.uk**, into your browser or use our Mobile Banking app.

- **Never transfer or withdraw money out of your account if you're instructed to do so for security reasons.**

  Fraudsters will call you pretending to be from the police, our fraud department or other legitimate organisations to gain your trust and tell you that your account is at risk of fraud. They'll convince you to transfer or withdraw your money to help keep it safe. Santander, the police or any other organisation will never contact you and ask you to move your money, for any reason.

- **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.**

  A fraudster could impersonate the person or company you're expecting to pay by sending an email, which will look genuine. They'll request an immediate payment or tell you they've changed their account details, meaning you'll actually be sending your money to a fraudster.

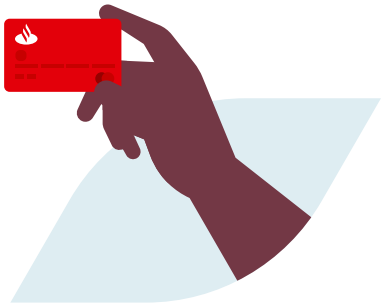
Along with our top tips here are some of the other signs to look out for and how to keep yourself secure:

- If you ever receive a message with a One Time Passcode (OTP) which you weren't expecting, call us immediately on **0800 9123 123** as it could be a sign of fraud.
- Make sure the details in your OTP message match the transaction you're completing. If it doesn't, don't enter the OTP and call us immediately.
- Don't rely on a caller's phone number to verify their identity. Fraudsters can 'spoof' a phone number to make you believe it's a genuine call.
- Before transferring your money to an investment make sure you have thoroughly researched the company and checked their details on the Financial Conduct Authority's website **fca.org.uk**.
- Never log on to your Online Banking whilst someone else is connected to your device as they may be able to access your accounts and move your money.
- Be aware of others around you when using your card and PIN and always keep your PIN secure.
- Your card and PIN should never be kept together, so if someone gets your card they can't also get your PIN.
- Keep your anti-virus security up to date to protect yourself from computer viruses and malware.
- When buying goods online, you should try to avoid paying by bank transfer. Look at the different payment options available that could offer you greater protection, such as a credit or debit card.

Remember, a genuine organisation will never rush you into taking action on your account. If you're ever unsure of what you're being asked to do, take your time and don't be rushed.

More information

As well as the information in this leaflet, you can also visit our online fraud and security pages at **santander.co.uk** to find out more about the different types of fraud and scams and to how protect yourself.



What we're doing to protect your accounts

Automated transaction monitoring

We're always monitoring your accounts looking out for any suspicious behaviour. If we spot something we'll try and contact you to check whether or not you recognise the transactions.

We use an automated system to contact you so we can get in touch as quickly as possible and may contact you by phone, text message or email.

Automated phone call

- You'll be asked to verify your name and date of birth and then we'll read out the transactions we need you to verify.
- If you don't recognise a transaction you'll be transferred to a member of our security team who'll be able to help you.
- If we can't reach you, we may leave a voicemail letting you know we called.

Interactive text message

- We'll send you two messages. The first is an introductory message to tell you that we need to check some activity with you and that we'll send the next message from a different number. We do this so that you can send a response to the message and tell us quickly whether you recognise the transactions.
- The next message will include the transactions we want to check with you. It will ask if you recognise them and to either reply 'Y' or 'N' to the message. We won't ask you to respond with anything else.
- If you reply 'N', we'll call you back as soon as we can. We'll also give you a number that you can call us on if you prefer.
- If you reply 'Y' we'll update our records and you can continue banking as usual.

Email

- If we send you an email, this will be to ask you to call us or tell you that we've sent you a text message.
- We won't include any transaction details or ask you to reply to the email

On some occasions we'll give you a 3 digit code in your voicemail or text message to enter into your phone when you call us back. This won't be used for any other purpose and we'll never ask you to tell anyone what it is.

Authenticating transactions

Some transactions that you complete online will require additional authentication, for this we may use a One Time Passcode (OTP) or ask you to verify this using your Mobile Banking app. When it's needed you'll see a prompt on screen asking you to open the app or to enter the code. OTPs will be sent by text message to your registered mobile number. You'll receive a new code for every request and you'll only be able to use it once.

When authenticating your transactions always remember:

- You must never share an OTP with another person. Not even with a Santander employee
- You should only enter an OTP if you've requested the transaction yourself
- If you receive an OTP message that you're not expecting, please call us immediately
- We'll never ask you to open the app or to enter or disclose an OTP to stop or cancel a fraudulent transaction.

Verified by Visa and MasterCard Secure (3D Secure)

Santander Secure, in partnership with Verified by Visa and MasterCard SecureCode, helps protect your card against unauthorised use when you shop online.

For your security you may, from time to time, be required to authenticate your payment with an OTP or with your Mobile Banking app.

Trusteer Rapport

We recommend you download Trusteer Rapport. It's free security software that works alongside your normal anti-virus software to give you more protection on your computer.

- It strengthens your online security by 'locking down' the connection between your computer, keyboard and Online Banking.
- It helps stop your data going to counterfeit sites, so you can be safe in the knowledge that only you are transacting on your account.
- It can also help identify and remove malicious software (malware).

How to download

Visit our fraud and security pages at **santander.co.uk** for further information and instructions on how to download the free security software.

Confirmation of Payee

When making a new payment or amending an existing payment we'll check the details of the person you are paying using the Confirmation of Payee service. This will help you be as sure as you can be that your money goes to the right place.

If the details don't match, we'll let you know. Before continuing with the payment you should contact the person you are paying to confirm the payment details.

You should do this using trusted contact information and not any contact details provided with the payment request.

Payment warning messages

When making a payment from your account we may give you some information about the potential scam risks associated with the type of payment you are making.

It's important you pay attention to this information and be honest with us about the reason for your payment, as this could help prevent you from losing your money to a scam.

In branch

If you visit a branch, you'll be asked to use your card in our Chip and PIN device. This helps us identify you as the account holder and reduces the risk of impersonation fraud.

- Once you've entered your PIN successfully, we can access any of your Santander accounts.
- For some transactions we need extra identification, so it's useful to bring your ID with you.
- We'll check your ID to confirm that it's a genuine document and that it's on our list of acceptable identification.
- If we can't verify the document you provide, you may be asked for more ID before we can complete your request.

Are your details correct?

So that we can get in touch with you as quickly as possible and so that you can continue to receive OTPs, it's important to keep your contact details up to date.

You can check and update the contact information we hold for you in Online Banking - My Details & Settings, by calling us on **0800 9 123 123**, **0800 731 6666** for business customers, or by visiting your local branch.

Reporting fraud

Please call us on 0800 9 123 123 or 0800 731 6666 if you're a business banking customer:

- If there are transactions on your account that you didn't authorise
- To report lost or stolen bank cards, log on details, statements or cheque books
- If you think your PIN, password or personal data may have been compromised
- If you believe you've been a victim of a scam or fraud, or are being targeted
- If your mobile phone provider has informed you that your SIM has been swapped without our knowledge

If you receive a suspicious email that appears to have come from Santander please forward it to **phishing@santander.co.uk** or if it's a text message **smishing@santander.co.uk**.

Reporting to Action Fraud

If you think you've been scammed or you're being targeted, you should also contact Action Fraud, a government organisation closely associated with the police.

- Use the online web reporting tool at **actionfraud.police.uk**
- Call **0300 123 2040** (text phone **0300 123 2050**).

TAKE FIVE TO STOP FRAUD™

Take Five

Take Five is an industry-wide campaign supported by Santander. It offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud.

takefive-stopfraud.org.uk

Santander is able to provide literature in alternative formats. The formats available are: large print, Braille and audio CD. If you would like to register to receive correspondence in an alternative format please visit **santander.co.uk/alternativeformats** for more information, ask us in branch or give us a call.

MISC 1755 APR 21 H