Santander

Protect yourself from fraud

Keep yourself safe from fraud and scams

We want you to be safe and secure when you bank with us. We have security measures in place to help with this. But there's a few things you can do too. Knowing how to use your accounts safely can help prevent fraud.

Keep our top tips in mind

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

  OTPs are used to verify online transactions. Only you should enter these to authenticate the request. We'll never ask you to share one with us in any circumstance. Any requests to do this will be fraudulent.

- **Never move money out of your account for security reasons.**

  Criminals impersonate bank staff. They also pretend to be the police and other trusted organisations. They'll tell you your account's at risk. To protect your money it needs to be moved to a new account to keep it safe. Any instructions like this are a scam. Always take time to double-check what you're being asked to do before acting. A genuine organisation will never rush you in to taking action.

- **Confirm all new payment requests or requests to change bank details.** Criminals can trick you into making payments.

  They do this by sending fake invoices or intercepting emails. Always confirm the receiving bank details. You should do this in person or on a publicly available number. Don't use the number given to you in the email requesting payment. This can lead to you checking with the criminal.

- **Complete extra checks to make sure the request is real.** Take time to do checks when making any payments.

  You need to make sure the payee and the request is genuine. You can read reviews, research companies or websites. You should also check the person or company is who they say they are. If it's for an investment, check the company is authorised. The Financial Conduct Authority have a register you can check. Their 'ScamSmart' tool can be used to help check if an investment is a scam or not.

- **Never allow anyone access to your computer following a cold call.**

  Criminals want to access your computer or devices. This is so they get control of your digital banking. They may ask you to download software. Or ask you to let them remotely log on. They may say they can help with computer or internet issues. Don't allow them access in this way.

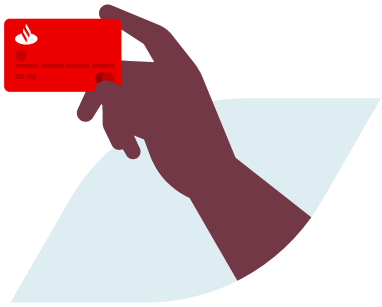
Most scams involve some form of impersonation. This is where someone pretends to be someone else. Criminals will impersonate anyone they think you trust. This could be a loved one or a friend. They could pretend to be your bank or the police. They'll tend to add a sense of urgency. This is to make you panic into sending money or sharing information. Always take time to think about what you're being asked to do.

Keep your personal and security information safe. You can do this by making sure you:

- Call us straight away if you receive an OTP (One Time Passcode) you aren't expecting.
- Check the OTP message matches the transaction you're doing. If it doesn't, stop and call us.
- Don't use caller ID to check a person is who they say they are. Criminals can 'spoof' a number to hide the real number they're calling from.
- Do thorough checks before transferring money to an investment.
- Never log on to digital banking while someone's connected to your PC or device.
- Keep your anti-virus software up to date. Complete regular device updates. This prevents viruses and malware.
- Keep your PIN and card separate. Be aware of who's around when you're using your PIN.
- Pay for things using the safest option available. Card payments, PayPal and 'buy now' options on websites offer the most protection.
- Avoid paying by bank transfer or cash. Especially for something you haven't seen in person.

More information

You can visit our fraud and security pages at **santander.co.uk**. Here you can find out more about the different types of fraud and scams. It also gives you information on how protect yourself.



What we're doing to protect your accounts

Automated transaction monitoring

We monitor your accounts using automated systems. These look for any suspicious behaviour.

We'll get in touch if we want to check something with you. To do this, we may use an automated service. This means we can speak to you quickly. Contact can be made by phone, text message or email.

Automated phone call

- You'll be asked to confirm your name and date of birth. Then we'll list the transactions we need you to verify.
- If you don't recognise a transaction, we'll need to talk to you.
- You'll be transferred to a colleague in our security team. You can then discuss the transaction in more detail.
- We may leave a voicemail if we can't get in touch.

Interactive text message

- We'll send you 2 messages. The first is an introductory message. It will tell you that we need to check some activity with you. And that the next message will come from a different number.
- The second message will include the transactions we want to check with you. It will ask if you recognise them. You need to either reply 'Y' or 'N' to the message. We won't ask you to respond with anything else.
- If you reply 'N', it means you don't recognise the transaction. A member of our security team will call you as soon as they 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. You can then continue banking as usual.

Email

- We can email you. The email may ask you to call us. Or it may tell you that we've sent you a text message.
- We won't include any transaction details in this message. We'll never ask you to reply to the email.

Sometimes we'll give you a 3-digit code. This may be in a voicemail or text message. We'll ask you to type it into your phone when you call us back. This won't be used for any other reason. We'll never ask you to tell anyone what it is.

Digital Payment Limits

Set your own payment limit for Online and Mobile Banking

You can set a payment limit in Online and Mobile Banking. This lets you control how much you can send from your account in one transaction. It only applies to digital payments from your personal accounts. Set your limit for any amount between £0.01 and £25000.

You should check your limit regularly. Make sure it's set at the right amount for you. Having a lower limit can help protect you from fraud.

Authenticating transactions

Sometimes your online transactions will need additional authentication. This is to make sure we know it's you making them. It provides extra security when you buy or make payments online. You can't authenticate a transaction to stop it leaving your account. So if you're asked to do this, it will be fraudulent.

When authentication is needed, you'll see a prompt on your screen. You can authenticate a transaction in 2 ways.

- We'll either send you a One Time Passcode (OTP) by text or email.
- Or we'll ask you to verify the transaction using your Mobile Banking app.

Criminals try to get around this process

They may ask you to share OTPs with them. We will never ask you to do this. OTPs shouldn't be shared with anyone. Not even Santander staff.

Criminals may ask you to confirm a transaction in the mobile app. You should only ever authenticate a transaction you've made yourself.

The message you receive will tell you details about the transaction. You should make sure this matches what you want to do. If someone tells you to ignore this information, this will be fraudulent.

If you receive an authentication request you weren't expecting, call us.

Trusteer Rapport

Malware is the short name for malicious software. It's used by criminals to get information or access to your accounts. Trusteer Rapport is a malware protection software. It's free, easy to install and simple to use. It will work with any existing security software to:

- let you know if you're using the bank's genuine website.
- provide a secure connection between your computer and the bank.
- identify malware and neutralise it.
- You can download this from our website santander.co.uk.

Confirmation of Payee

We can check the bank details of the person you're paying. This is done through the Confirmation of Payee (CoP) service. A CoP check can help you understand whether your money is going to the right place. Criminals may try to trick you in to making payments where the details don't match.

We do a CoP check when you make a new payment. We also do it when you change an existing payment. If the details don't match, we'll let you know. This means you can contact the person you're paying to check the details. You should do this before sending any money.

Payment warning messages

Criminals will try to get you to make payments. This is to get you to send your money to their accounts. We want to protect you from this. One way we do this is through scam warnings. These are given in our branch, telephone and digital channels.

We give you information about the potential scam risks. These are specific to the type of payment you're making. It's important you're honest with us during these conversations. This is so we can give you the right information.

Transactions 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. It reduces the risk of someone pretending to be you.
- For some transactions we need extra identification. It's useful to bring your ID with you. We'll check your ID to make sure it's a genuine document.
- Sometimes we can't verify the document you provide. If this happens, we'll ask for more or different ID. We'll need this before we can complete your request.

Your contact information

It's vital you keep your contact details up to date. This is in case we need to get in touch with you. It also allows you to receive OTPs. You can check and update your contact information using Online Banking. Just go to 'My Details & Settings'. Or you can call us or visit your local branch.

Reporting fraud

It's important you contact us with any fraud concerns. This helps us protect your money and your information.

For personal accounts, please call 0300 9 123 123 or 0800 313 4321 (freephone)

You must call us if:

- There's transactions on your account you don't recognise.
- You need to report something lost or stolen. This includes bank cards, log on details, statements or cheque books.
- You think your information has been compromised. This includes your PIN, password or personal data.
- You believe you've been the victim of a fraud or scam.
- Your mobile phone provider has told you your SIM has been swapped.

You should report suspicious emails and text messages to us. This means we can take steps to prevent fraud.

- Emails should be forwarded to **phishing@santander.co.uk**.
- Text messages should be forwarded to 7726. And emailed to **smishing@santander.co.uk**.

For Business Banking accounts, please call 0330 123 9860 or 0800 011 3414 (freephone)

Action Fraud

Action Fraud is a service run by the City of London Police. They work alongside the National Fraud Intelligence Bureau (NFIB). It's the UK's national reporting centre for fraud and cybercrime. Use the tool to report fraud at **actionfraud.police.uk**. Or call **0300 123 2040** (text phone **0300 123 2050**).

159 – Stop Scams UK

159 is a phone service offered by Stop Scams UK. You can dial 159 and be connected to Santander. It's useful if you receive an unexpected or suspicious call. You can call just one number and know you'll be connected to the right place.

Take Five

Take Five is an industry-wide campaign supported by Santander. It offers straight-forward and impartial advice on fraud. This can help you protect yourself from preventable financial fraud. Visit **takefive-stopfraud.org.uk**.