Fraud and scams

Over 40% of crimes in England and Wales are to do with fraud and scams.

What we're doing

We help keep your accounts secure in many ways.

- We monitor accounts for signs of fraud. If something doesn't look right, we'll contact you to talk about it.
- We use Strong Customer Authentication (SCA). This adds extra layers of security to online transactions.
- We provide industry-trusted technology. It secures your identity and finances when you access your accounts online.
- We'll automatically log you out if you forget.
- We offer a variety of user management and payment controls. These give you flexibility in maintaining your security.
- We only allow a limited number of incorrect login attempts. After this, we'll block access to Santander Connect. This protects it from any unauthorised access.

What you can do

You can help keep your business safe from fraud and scams through some simple steps.

- Make sure all staff are regularly trained on fraud and scams. Especially those who request or support the making of payments. It's important everyone understands the potential risks to your business. All staff need to know how to spot something suspicious. And understand how to keep the business safe.
- Create an open and risk-aware culture where people are able to raise concerns quickly.
- Make sure your business has robust payment processing procedures and controls. They should include dual authorisation, payment authorisation limits and password management policies.

Our top security tips

- **Never** share any passwords or token codes with anyone. Not even a Santander employee.
- **Never** use the mobile app to authenticate a transaction you didn't select yourself in Online Banking.
- **Don't** allow anyone to remotely access your computers or devices.
- **Don't** trust the caller ID. Numbers on phone calls and SMS messages can be spoofed. This means it looks like a genuine company or person is calling. To validate any Santander calls, visit our website for the genuine phone number.
- **Check** every new payment request in person or over the phone. This includes changes to existing payments. Don't use the contact details in the payment request. This may lead to you making the check with the criminal.
- **Never** disclose sensitive or security details over the phone, in emails or in any other message formats.

TAKE FIVE TO STOP FRAUD™

Contact us straight away if you're concerned about anything. Remember you can visit: **www.santandercb.co.uk/support/fraud-prevention**

CCB MC0234 MAY 24 IPG CD