Fraud and scams

1 in 4 businesses are affected by fraud. We want to let you know how you can keep your accounts safe, and reduce the risk to your business.

What we're doing

We help to keep your accounts secure in a variety of ways.

- We monitor your accounts. If something doesn't look right, we'll contact you.
- We use Two-factor authentication for online transactions.
- Industry-trusted technology that secures both your identity and finances.
- Provide secure online sessions whilst you bank online.
- Session timeouts that will automatically log you out if you forget to.
- Offer a variety of user management and payment controls to add further flexibility in maintaining your security.
- Log in protection, we'll secure your online banking after a number of incorrect attempts to protect against any unauthorised access.

What you can do

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

- Ensure **all staff are regularly trained** on fraud and scams, especially those who request or support the making of payments. It's everybody's responsibility and this means they will always understand the risks to your business, how to spot something suspicious and how to keep the business protected.
- Create an **open, risk-based culture** and have procedures in place for staff to escalate any concerns appropriately.
- Make sure your business has **robust payment processing procedures and controls**, including dual authorisation, payment authorisation limits and robust password management policies. This means you can give your business an increased chance of preventing fraud or scam activity.

Key prevention advice

- **Never** share a token code with anyone, not even a Santander employee.
- **Never** use the mobile app to authenticate a transaction you've not chosen yourself.
- **Never** use caller ID to validate contact – numbers can be 'spoofed' (imitated) to be the same as genuine ones.
- **Never** be afraid to hang up and call us back using the number from our website.
- **Never** disclose sensitive or security details over the phone, in emails or in any other message formats.
- **Always** validate payment requests on a known phone number or in person first. The check must not be made using the number provided in any emails, WhatsApp or text messages requesting payment as this can lead to the check being made with the criminal.

Contact us immediately if you think you've been a victim of a fraud or scam. Remember you can visit: **www.santandercb.co.uk/support/fraud-prevention** for more advice.

TAKE FIVE TO STOP FRAUD™

CCB MC0234 JUN 22 H