Suspicious emails, texts, and calls: what to look for — and what to do next

Did you get a suspicious email, text message, or phone call from someone pretending to be your bank? If it raised your alarm bells — and as a result you didn't interact with it, share information, or send money — great work!

To keep yourself safe, get familiar with the most common tactics used by scam artists — and learn how you can fight back by reporting these attempts to Santander.

Step 1: Keep recognizing the warning signs

Emails: what to watch out for

- Requests to share your password, an OTP (one-time passcode), or your personal details: "Unusual account activity detected — enter your information to confirm"
- Urgent messages pushing you to sign in, with a button or link: "Your account will be locked unless you sign in now"
- Attachments you don't expect, or requests to 'enable macros' or other technical items: "You have a secure message — open attachment"
- **Notice the little details** — scam emails often contain spelling or grammatical errors
- **Always check the sender's email address** — scam emails often come from sources that seem almost right, but when you look closely you see extra letters in the name, swapped characters, or unfamiliar email domains
- **Never open attachments or click links** from suspicious emails

Text messages: common scam clues

- Demands to confirm actions outside of Santander Online Banking or our Mobile app: "A transfer is pending — visit <unfamiliar website URL> immediately to confirm"
- Urgent requests to click on shortened or unfamiliar web links: "Your account is on hold — tap here to restore access"
- **Notice the little details** — scam messages often contain spelling or grammatical errors
- **Always look at the source** — scam messages often come from sources that look almost right, but when you examine them closely you see they're not actually from Santander (look for extra letters or swapped characters in the name, or an unfamiliar email domain)
- **Never click links** from suspicious text messages

Phone calls: when to be suspicious

- Anyone calling to ask for your account password, your PIN, or an OTP (one-time passcode): "I'm calling from Santander — tell me the code we just sent you"
- Requests for sensitive information over the phone: "This is Santander and we need to verify your identity — tell us your account details"
- Requests to install software or give the caller remote access to your account: "Install this app so we can help secure your account"
- **Note: Santander will NEVER call you to ask for this information**

Step 2: Check your account

Take a few minutes to review your Santander Bank account either online or on our Mobile App, and make sure you don't see any activity or transactions you didn't authorize. If you see something wrong and suspect fraud? **Call us right away at 1-877-906-7500.**

Step 3: Report the suspicious message

By sharing these scam attempts with us, you can help us to identify new fraud trends and develop strategies to fight back. Please send all suspicious messages to reportabuse@Santander.us and be sure to use "Suspicious message report" in your email subject line.

Here's how to send us each kind of message:

- **Emails:** please send us the suspicious email as an attachment, instead of forwarding it to us directly. Be sure to include the suspicious email's subject line, any reference numbers included, and any links or attachments from the original email (but do NOT click on them).
- **Texts (SMS):** Attach a screenshot and/or paste the message into the email body. Be sure to include any links (but do NOT click on them).
- **Phone calls:** Be sure to let us know the phone number the suspicious caller used; the date/time of the call; and what they asked you to do.

When you contact us, be careful NOT to include the following:

- Your full Santander Bank account or credit card number
- Your PIN or any OTP that was actually sent to you by Santander Bank
- Your full Social Security Number

You won't receive a reply to your email, but rest assured that your report will make an important difference in helping us to shut down fraudsters.