Starling Bank

TAKE FIVE TO STOP FRAUD™

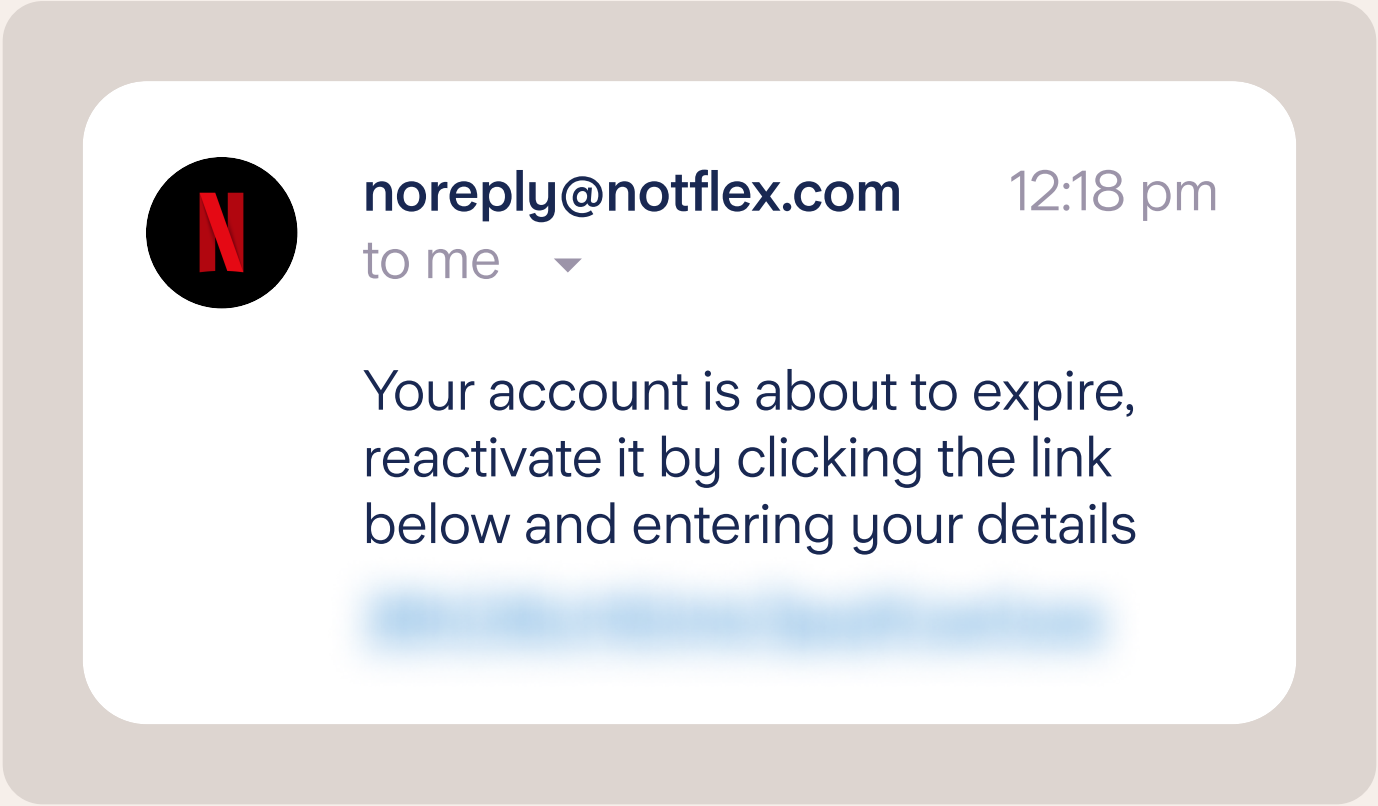
Keep yourself safe from

Phishing and Smishing Messages

Fraudsters will impersonate genuine companies and send messages to victims to steal their personal or financial information. These are known as phishing messages when sent by email or smishing messages when sent by text.

Emails may appear to come from an address similar to the impersonated organisation and texts may come from spoofed phone numbers (when a number looks like it belongs to a genuine company). They will contain links to fake websites, where the intention is to harvest information like login details, card information or personal information. This information will then be used to scam you or steal money directly from your bank account. Links can also download malicious software onto your device.

The messages you receive in phishing or smishing messages may ask you to act quickly to “secure your bank account”, “prevent hackers accessing an account” or “pay a delivery fee”. Others may promote “limited time offers” to entice you into clicking links.



Top tips for avoiding phishing and smishing messages:

- Always question any messages containing links. Instead of clicking, go to the company’s website directly to log in or find the offer. This can be done by typing the company’s address into your browser if you know it (e.g. type ‘starlingbank.com’ into the address bar) or using a search engine.
- No company would ever ask you to log into your account to protect it from hackers or send you a link to confirm your login details out of the blue.
- Delivery companies will never text you to ask for a payment to deliver items. Always go directly to the delivery company’s website to check the progress of your package.
- If you receive a link in an email and you are viewing it on a computer, hover your mouse over it to check if the web address matches what you think it should be.
- Report any suspicious emails to report@phishing.gov.uk and forward any texts to 7726 for them to be investigated. This could prevent others being targeted.

If you think you’ve engaged with a fraudulent message, contact your bank straight away to advise them your personal, financial or login information may be compromised. Be aware that the scammers may contact you pretending that your money is at risk because of the message you responded to and ask you to move money or make payments to keep it safe. A genuine bank or organisation will never do this.

Find out more by reading our articles on **Phishing**, and **Delivery Scams**, or learn **What To Do If You’ve Shared Sensitive Information** on the National Cyber Security Centre's website.

If you’re ever unsure about a payment you've been asked to make, or already made, get in touch with us on your app or by calling 159. We’re here to help you. You might also want to speak to Victim Support, an independent charity that can provide support to victims of crime and traumatic events. Their **helpline** is open 24/7.