





Keep yourself safe from

Safe Account Scams

When a criminal convinces you that your bank account is not safe and then persuades you to move money or approve payments, this is known as a safe account scam. The fraudsters will impersonate banks, the police, the National Crime Agency, or even an internet provider (under the pretence that your internet connection is compromised). Criminals will tell victims that if they don't act immediately, all their money will be lost. This is done in an attempt to pressure them into making a quick decision.

These scams sometimes start when the victim responds to a fraudulent text or email (known as smishing or phishing messages), tricking them into sharing personal and/or financial information. This information can then be used by the fraudsters to convince you that you're speaking to a genuine organisation when they call you.

Scammers can also try to convince you that your real bank is under investigation and tell you to lie if your real bank calls you, with the idea that the 'investigation' needs to be kept secret. This encourages victims not to tell the truth if asked for the reason for a particular payment. The scammers may also ask you to download remote access software onto a computer or mobile device, so that they can access your bank account on your behalf.

Your bank account is being hacked! Move your money out of your account to keep it safe.

Top tips for avoiding safe account scams:

- Starling, or any other bank, will never ask you to move money into a new account to keep funds 'safe', by any payment method. Neither will law enforcement agencies or internet providers. If you get a call like this, hang up immediately and call us on 159. This will ensure that you're actually speaking to Starling.
- Fraudsters can fake phone numbers to make their calls or text messages seem genuine. If you're unsure about a call you've received, hang up and phone the trusted number found on the organisation's website to confirm if the call or text you have received is genuine.
- If you received the call on a landline, make further calls from a different device as fraudsters may keep the original line open.
- If you've been told about an overpayment or loan into your account that you're not entitled to, make sure to check your account independently using your bank app or online banking. If you see a payment in your account you don't recognise, hang up the call and call us immediately.
- Forward suspicious text messages to 7726 to report spam texts directly to your mobile provider.

the <u>Take Five</u> or <u>The Met Police</u> websites.

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.

Find out more by reading our article on Impersonation Scams, or visiting