Starling Bank

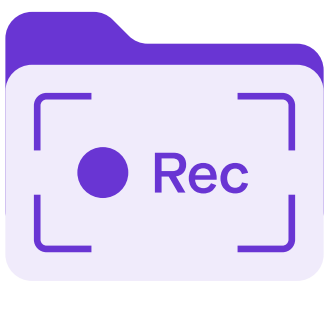
TAKE FIVE TO STOP FRAUD™

Keep yourself safe from

Remote Access Apps

Remote access apps - sometimes called screen sharing applications - or software like Teamviewer or Anydesk, allow another person to view your screen or control your device.

Criminals can trick you into downloading one of these apps. The fraudsters might impersonate a bank, financial adviser, or internet provider and say that they need access to help protect your money, help you invest or fix your computer. But once you've downloaded the software, they'll be able to see any login or personal details that are stored on your device, and use this information to steal your money.



Top tips for avoiding remote access scams:

- A genuine company will never call out of the blue and ask you to download a remote access app. If someone asks you to do this, hang up immediately.
- 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.
- Legitimate financial advisers won't use remote access applications. Make sure anyone helping you invest is listed on the **FCA register**.
- Stay calm - criminals will pressure you into acting quickly, so hang up and speak to a family member or friend before downloading anything onto your phone or computer. You can also contact your bank for advice by calling 159.

If you've given a criminal access to any of your devices:

- Uninstall the app or software immediately - search on Google for step-by-step instructions on how to do this on your device if you're not sure.
- Once you're sure the software is uninstalled, update any passwords that the criminals might have seen.
- Let your bank know if you think your account information may have been accessed.
- Check your credit report regularly to make sure your personal information isn't being used to apply for loans or credit cards.
- Report the incident to **Action Fraud**.

Find out more by reading our article on **Remote Access Software Scams** and on **The FCA'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.