scam share

spotlight on...

Bank Scams

Scottish consumers regularly receive scam calls and text messages, supposedly from their bank, through which scammers try to obtain their account details.

what do bank scams look like?

The aim of most scam calls and text messages is to obtain your bank account details or to persuade you to transfer money to a scammer's account. Common scams may say:

This is your bank's fraud department. Your account has been compromised and you will need to transfer funds to a safe account.

There has been suspicious activity on your bank account and it is temporarily on hold until a verification process is performed. Click on this link to verify the activity...

A payment of £500 has been transferred overseas from your account. Press 1 to speak to an advisor to verify this transaction.

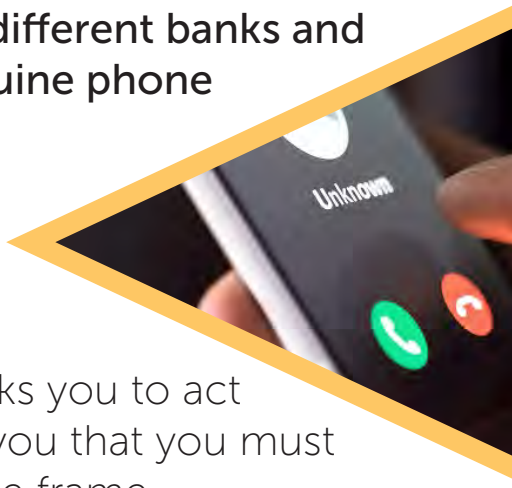
A new payee request has been submitted. You can authorise or cancel this request by clicking on this link...

You have authorised a payment to Joe Bloggs. If this was NOT you, click on this link to update your security details

how can I tell if a message related to my bank is a scam?

Scam messages appear to come from a number of different banks and often use number spoofing to clone the bank's genuine phone number.

Your bank will never cold call and ask you to move money to another account.



Be suspicious of any unexpected phone call or text message which appears to be from your bank and asks you to act urgently to avoid losing money. Fraudsters often tell you that you must provide your details or a payment within a certain time frame.

what should I do if I get one of these messages?

If you receive an unexpected message from your bank and are unsure if it is legitimate, **contact your bank using their official number.**

Don't give out any personal or banking details to a cold caller, even if they appear to know some of your details already.

Don't click on links in unexpected emails or texts - they may take you a cloned website which will ask for your personal and bank account details.

Do not press 1 or follow any other instructions given in an automated message.

Contact your bank immediately if you think you may have made a payment to a scammer or if you are worried that a fraudulent transaction has been made from your account. Use the phone number on your bank statement or a publicly listed number. To ensure that you are disconnected from the cold caller, phone another number such as 123 before phoning your bank or call them from another phone.

Report all scams to **Advice Direct Scotland** using their free consumer helpline: **0808 164 6000**

If you have lost money or are worried that you have given your bank details to scammers, contact **Police Scotland on 101**.

Find more information and advice on avoiding scams:

Advice Direct Scotland - www.consumeradvice.scot
Police Scotland - www.scotland.police.uk/keep-safe
Trading Standards Scotland - www.tsscot.co.uk/latest-scams

Trading Standards Scotland