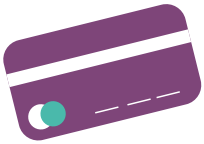
scam share

spotlight on...

Bank Scams



Scam calls and text messages, supposedly from your bank, saying there is an issue with your account or asking you to assist with a 'fraud investigation'.

The aim of these messages is to obtain your bank account details or to persuade you to transfer money to a scammer's account.

Common Scams

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...

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

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

I work for your bank's security team and we're investigating counterfeit notes being used by some staff. Could you assist us? You'd just need to withdraw £200 in cash, then hand it to a police officer who will visit your house.

Avoid Bank Scams

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

Your bank or the police will never call to ask you to verify your personal details or PIN by phone or offer to pick up your card by courier

They will not contact you out of the blue to participate in an investigation in which you need to withdraw money from your bank or to purchase high value goods for safe keeping

Your bank will never send a courier to your home to collect your card/PIN - any requests to do so are a scam

They will never ask you to withdraw money to hand to a police officer

If you receive a suspicious call supposedly from your bank, hang up, wait a few minutes to clear the line and call your bank on a number you know to be genuine, such as the one on the back of your card

Never give any details to a cold caller, even if they appear to know some of your details already.

Report bank scams

Report all scams to **Advice Direct Scotland** on **0808 164 6000** or via **scamwatch.scot**

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

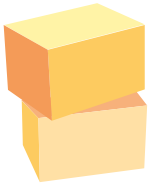
Find out more:

www.tsscot.co.uk/scamshare

scam share

spotlight on...

Delivery Scams



Scam emails and texts related to shipping or deliveries, which appear to have been sent by Royal Mail or other delivery companies.

The aim of these messages is to obtain your personal and payment information, often by asking you to click a link leading to a website with official-looking branding and logos

Common Scams

Your package has an unpaid shipping fee. Pay now by tapping on this link... If not paid a return to sender will be requested

Your driver Joe Bloggs was unable to deliver your parcel today. Click here to reschedule your delivery...

We're sorry to let you know that your package which arrived today will be sent back. This may happen when the receiver's address is incorrect. To redeliver please fill out this form...

Due to damage to the outer package in the process of transportation your address information was lost. Please update the delivery address within 12 hours via this link...

Your package has been in storage for an extended period of time due to a damaged shipping label. Please use this link to pay the storage fee of £50.00 within the next 72 hours...

Avoid Delivery Scams

Legitimate parcel delivery services will not contact you unexpectedly to ask for personal or payment details

If you are expecting a parcel, track the delivery on the company's official website

Don't click on links or use contact details provided in an unexpected message

Check the message carefully

Scam emails often use impersonal greetings such as 'Dear Customer' and they may contain spelling and grammatical mistakes.
They may ask you to act urgently in order to avoid losing a package. Be suspicious of any message which appears to be from an official company or organisation and tells you that you must provide your details or a payment within a certain time frame

Royal Mail do not collect shipping costs by email or text

If you need to pay an extra delivery charge, they will post a card through your door to let you know

Report delivery scams

Report all scams to **Advice Direct Scotland** on **0808 164 6000** or via **scamwatch.scot**
You can report Royal Mail scams at **reportascam@royalmail.com**
If you have lost money or are worried that you have given your bank details to scammers, **contact your bank and report it to Police Scotland on 101**

Find out more:

www.tsscot.co.uk/scamshare

scam share

spotlight on...

Prize Draw Scams

Fake competitions, prize draws, voucher giveaways or surveys on social media or in emails, which appear to be linked to well known companies.

The aim of these messages/adverts is to encourage you to click a link leading to scam websites which are designed to harvest your details.

Common Scams

We're giving away 100 luxury hampers worth over £1,000! To be in with a chance of winning click here and answer a couple of quick questions...

You have been chosen to participate in our Loyalty Program for FREE! It will only take you a minute to win a fantastic prize - click here to get started...

Congratulations! To thank you for your loyalty we are offering you the opportunity to win a £200 gift voucher. This is your last chance to win...click here to find out how to claim your prize...

You have been selected to participate in an anonymous survey about your experiences with our store. Complete this short survey to receive exclusive reward offers including vouchers...

Avoid Prize Draw Scams

Before taking part in a survey/competition which is supposedly being run by a well-known brand, look at their official website and social media channels to see if it is genuine

Be wary of quizzes or surveys on social media which ask for personal details

Think carefully about what information you are putting online. You don't know who is accessing the information you enter and what they could use it for

Check the spelling, grammar and T&Cs

Scam offers or giveaways often contain small mistakes and unusual wording. They don't usually list basic terms and conditions such as deadline dates or details on how winners will receive their prize

Remember that you cannot win a competition or prize draw you didn't enter

If you receive unsolicited WhatsApp messages, emails or texts offering prizes or deals, do not click on any links or open any attachments and never enter any personal or banking details.

Report prize draw scams

Report all scams to **Advice Direct Scotland** on **0808 164 6000** or via **scamwatch.scot**
You can forward suspicious emails to **report@phishing.gov.uk**
If you have lost money or are worried that you have given your bank details to scammers, **contact your bank and report it to Police Scotland on 101**

Find out more:

www.tsscot.co.uk/scamshare

scam share

spotlight on...

TV Licensing Scams

Scam emails and text messages which appear to have been sent by TV Licensing, copying their branding and logos.

The aim of these messages is to encourage you to click a link which leads to a copycat TV Licensing website where you're asked to enter your details.

Common Scams

Today is your last day to remain licensed. You won't be covered if you let your licence expire. Your bank has declined the latest Direct Debit payment. Click here to pay now...

Due to outdated TV Licence account details your account has been flagged and it will be suspended if you fail to respond to this notification. To update your account you will need to tell us your personal details, payment method and provide official proof of your identity.
Click here to update and verify your account details...

Oops! Something went wrong with your payment. We're sorry to let you know that your TV Licence could not be automatically renewed. If you don't keep up with your payments we may be forced to cancel your licence or pass your details to a debt collection agency. Click here to make a payment...

Avoid TV Licensing Scams

TV Licensing have confirmed that they will only message customers about payments if they have missed one.

They will not ask you to provide personal or card details until you have signed in on their official website: **www.tvlicensing.co.uk**.

Check the sender

Genuine TV Licensing emails are sent from **donotreply@tvlicensing.co.uk** or **donotreply@spp.tvlicensing.co.uk**. They will include your name and/or part of your postcode. If the email begins with 'Dear Customer' or Dear Client' it may be a scam.

Be suspicious of any unexpected message which appears to be from an official organisation and says you must provide details or a payment within a certain time frame

Only criminals will try to rush or panic you - don't feel guilty about refusing or ignoring requests if you are not sure about the sender's identity

Never click on links in unexpected emails

If you are unsure if a message about your TV Licence is genuine, sign into your account at **www.tvlicensing.co.uk/yourlicence**

Report TV Licensing scams

Report all scams to **Advice Direct Scotland** on **0808 164 6000** or via **scamwatch.scot**
You can forward suspicious emails to **report@phishing.gov.uk**
If you have lost money or are worried that you have given your bank details to scammers, **contact your bank and report it to Police Scotland on 101**

Find out more:

www.tsscot.co.uk/scamshare