Citizens Advice Halton

Scam Awareness Week 21st- 27th October 2024

Top tips to avoid falling victim to a scam

Here are 5 quick tips to help identify scams online for Scams Awareness Week:

- **Too good to be true offers**: If something promises a deal or prize that seems unrealistic, it's likely a scam. Be sceptical of offers that sound too perfect.
- **Stop and Think:** Scams often pressure you into quick decisions by using phrases like "act now" or "limited time offer." Be cautious if something feels rushed. Genuine companies won't mind you taking your time to think about it.
- **Look for spelling and grammar mistakes**: Many scam messages have poor spelling or unusual sentence structures that stand out from legitimate communications.
- **Check for personal information requests**: Legitimate companies rarely ask for sensitive information (like passwords or bank details) via email or message. Always double-check with the official website or contact method.
- **Check the sender's email or URL**: Scammers often use addresses that look like real ones but have slight differences. Always inspect the domain name carefully and if in doubt contact the company directly using their website or official telephone number.

Common Scams

Telephone Scams

These are one of the most common scams in the UK.

This is when someone calls you up unsolicited to tell you about a fault or other problem with something you use.

The scammer will normally offer to fix the issue for a small fee.

Common examples are callers reporting that you have a virus on your computer, trying to sell energy deals or reporting issues with your banking.

Lifeline Scam

Vulnerable Halton residents received calls from someone reporting to work for the Lifeline service, saying that the emergency button on their equipment was faulty and needed replacement for a small fee of £300. There was nothing wrong with the equipment. This is a type of telephone scam.

If you are unsure or if something doesn't sound right just end the call.

Authorised Push Payment Scams

Victims are encouraged to make large transactions directly from their own bank accounts, often over several transactions

There are lots of versions of this scam, such as;

- Romance Scams – fraudsters build up trust and affection over time and use this to encourage their victim to transfer sums of money to them.
- Investment Scams – fraudsters promote a quick win investment (e.g. bitcoin). Victims will often invest small amounts and see immediate returns which encourages them to invest further.
- Auction Scams – fraudsters offer for sale a product that never existed.

The common theme is that the victim authorises the payment.

From the 7th October 2024, transactions made by Faster Payments (used for mobile and online banking) or CHAPS (same day transactions of high value – often used in home buying) will benefit from additional protection.

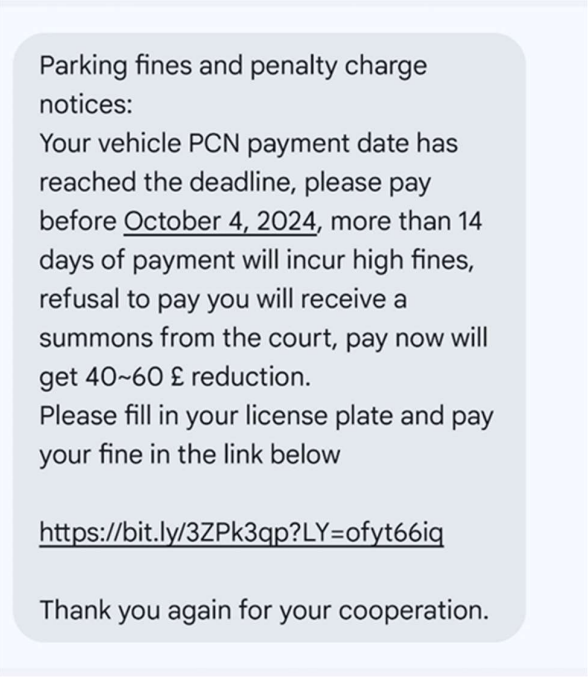
- Banks should refund losses up to £85,000 (they can take a £100 excess for taking this step in some cases)
- In most cases refunds should be received within 5 working days.

If you think you have been the victim of APP Fraud what should you do?

Call your bank immediately – tell them what has happened, if they can't stop the transaction they may be able to put a block on further payments.

Report the fraud – **You can contact Action Fraud on 0300 123 2040 or online at https://www.actionfraud.police.uk/** - they will give you a crime reference number which may help when talking to your bank.

Parking Scams



Parking fine text scams

If you have received a text message asking you to pay for a penalty charge notice (PCN) that has been issued by the Council. This will be a scam and you should ignore the message and do not click on any links within the message

Report a scam text at https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-text-message

Parking QR Code Scams

Scammers place fake QR codes on parking meters, to collect your payment details. This can also lead to large fines for unpaid parking to the official company.

- Check that the QR code has not been stuck over an existing sign
- Ensure the URL the code opens has a padlock sign
- Check the website belongs to the company you expect

If you've lost money or have been hacked as a result of clicking on links in text messages or inputting your details via QR codes you can:

Report via www.actionfraud.police.uk or call 0300 123 2040 (in England, Wales or Northern Ireland)

Parcel Delivery Scams

In the lead up to Christmas Parcel delivery scam messages are common. You may receive a text or email, impersonating a genuine company. Be alert for requests such as:

- A message asking for a fee to redeliver a parcel.
- A package you've sent will be returned, as the address was incorrect.
- A company tried to deliver a package, but you were out. Often this scam will include a link to schedule redelivery.
- A parcel isn't going to be delivered unless you download an app. These apps can contain spyware to capture your personal details when you next use them.

These messages can be difficult to tell apart from a real text or email.

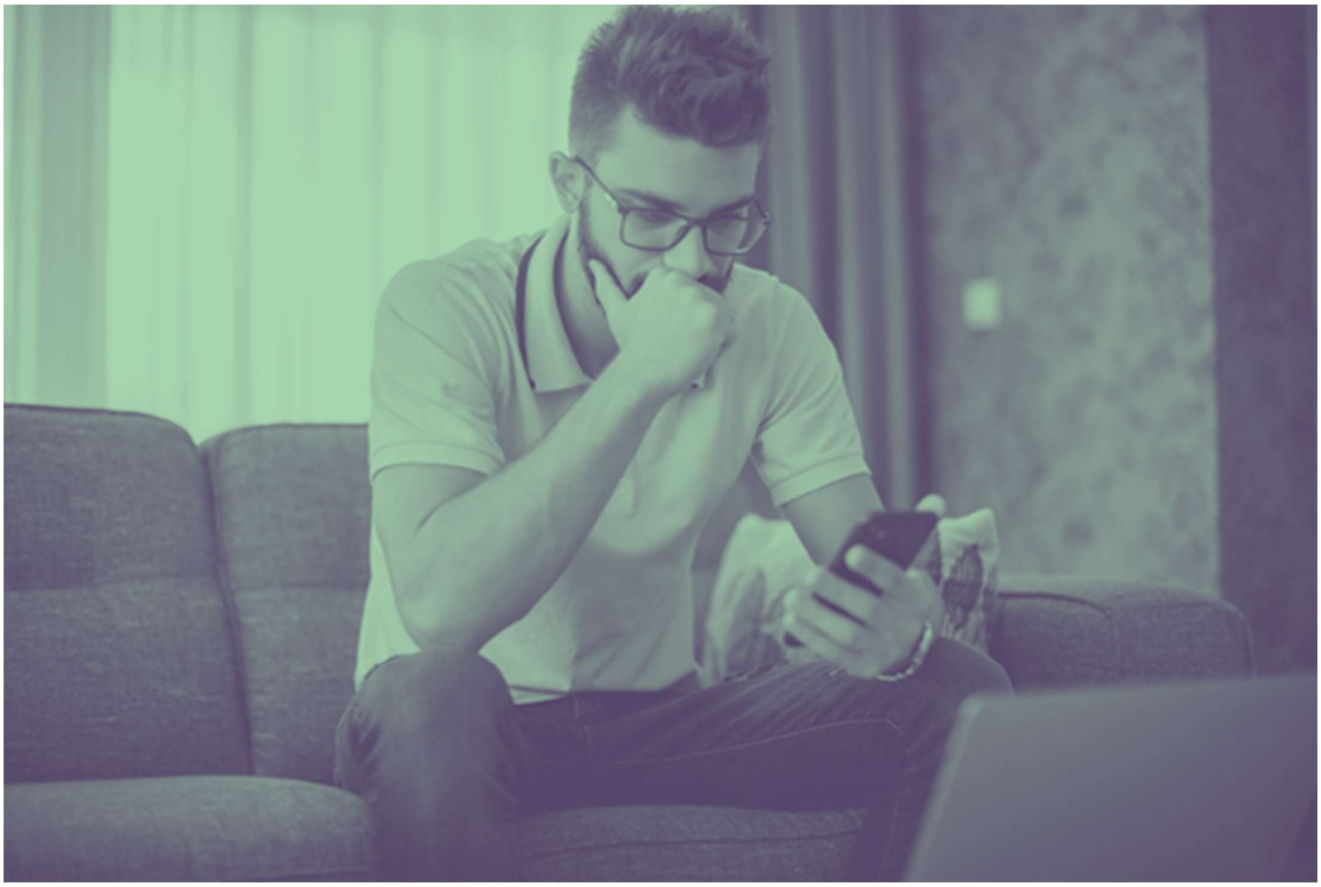
Here are some tips to avoid parcel delivery scam text messages:

- Check the number the scam message will often be from an ordinary mobile number
- They try to rush you using phrases like "act now" or "prompt action"
- Parcel details are vague and not tell you where it is from
- Spelling and grammatical errors check for mistakes
- Don't click links
- Check the domain name
- Contact the business

If you think you've already fallen victim to a scam, you can:

- Contact your bank and inform them of the situation.
- Run a full scan with antivirus software.
- Change your passwords on the account and any others that use the same password.
- Report it as a crime to Action Fraud

If you think you have been the victim of a scam you can find more information about what to do next at; https://www.citizensadvice.org.uk/consumer/scams/what-to-do-if-youve-been-scammed/



Further support and information:

You can find further information about scams on the Citizens Advice website at:

https://www.citizensadvice.org.uk/consumer/scams/

Or call the Consumer Service helpline on 0808 223 1133.

Free, confidential advice.
Whoever you are.

We help people overcome their problems and campaign on big issues when their voices need to be heard.

We value diversity, champion equality, and challenge discrimination and harassment.

We're here for everyone.

Adviceline freephone number: 08082 787 956.

Contact us online: https://haltoncab.org.uk/

haltoncab.org.uk

Published October 2024

citizens advice Halton