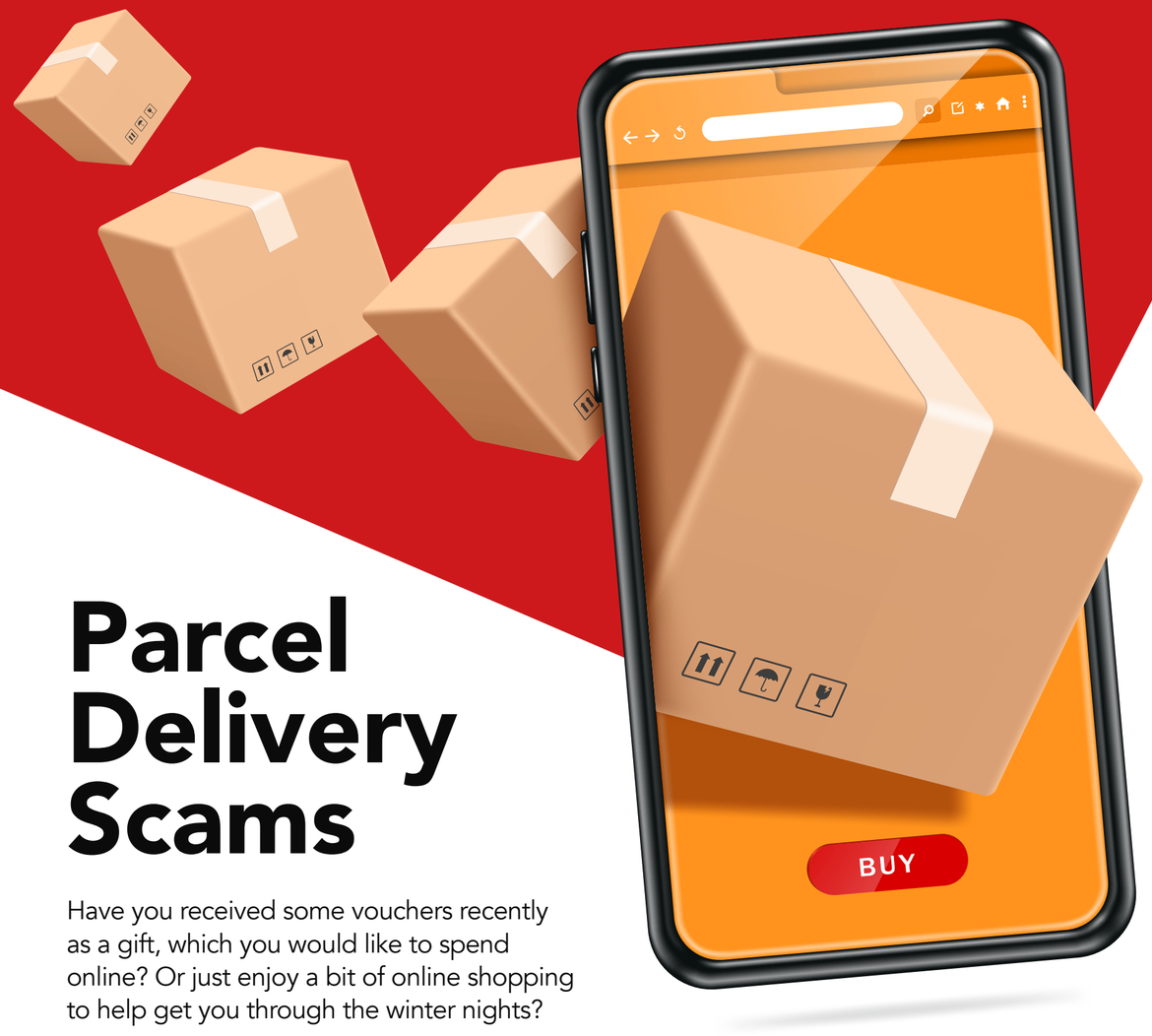


Parcel Delivery Scams

Have you received some vouchers recently as a gift, which you would like to spend online? Or just enjoy a bit of online shopping to help get you through the winter nights?

Online shopping can be extremely convenient. But it's important to be very careful of any texts or emails you receive from companies notifying you that they've been unable to deliver your latest order. This could be a scam!

In an age where we all want things instantly, the delay of a delivery can be incredibly frustrating. Often, we will do anything for an order to be with us as soon as possible. This frustration and impatience are what criminals of this scam thrive on and look to target.

As part of its Scams Awareness campaign, research from Citizens Advice* in the first half of 2023 found that parcel delivery scams were by far the most common scam faced by the public.

49% of people targeted by scammers had been on the receiving end of a malicious parcel delivery scam.

What are parcel delivery scams and how do they work?

Parcel delivery scams are messages that pretend to come from well known delivery companies such as DPD, Royal Mail or Parcelforce. The content, which is usually delivered via text message or email, may say that your package is delayed or will require a small payment to be delivered. These messages can often be difficult to tell apart from a real text or email.

These messages will typically contain a link which will send you to a fake website, designed to look like it belongs to a genuine delivery company. On this website, you may then be asked to make a small payment, as well as providing your personal information (name, address and contact details) to 'reschedule your delivery'.

Not only will you be out of pocket paying this pretend fee, but with your personal information provided, some criminals may go further by trying to process payments on your card. They will then call you pretending to be from your bank, claiming that there's been unusual activity on your account. Scammers can sound very convincing, quoting your email and card details back to you. They may then try to persuade you that your bank account is no longer safe and that you will need to send your balance to a new account they've created for you.

Alternatively, these texts or emails may also encourage you to download an app, stating your parcel will not be delivered unless you do so. The app is in fact malicious and contains spyware. If installed, it can steal your banking details, passwords, and other sensitive information.

Remember: no bank will ever ask you to move your money to keep it safe.

As described on page 5 – delivery scams are two prime examples of:

Phishing

Phishing is where a fraudster will send an email which appears to be from a legitimate company, attempting to obtain personal details from you.

Smishing

Just like vishing, fraudsters contact you by phone but instead of a phone call it is done using text messages where you are usually asked to follow a link or call a telephone number.

How to spot a delivery scam

Check carefully

A scam text message will often arrive as a mobile number (i.e 07123 456789) rather than from an official source or company.

Emails can also be sent. If this is the case, check the sender email address thoroughly. Scammers will often copy an official email address but make a very small amendment (for example, swapping an S with the number 5) to make it appear genuine.

They try to rush

A scam will often try to get you to act quickly, ensuring you don't have much time to think about what you are doing. If a message has a deadline set, this is usually suspicious.

Lacking details

Delivery scams are often vague and don't specify what's inside the parcel or where it is coming from.

Spelling errors

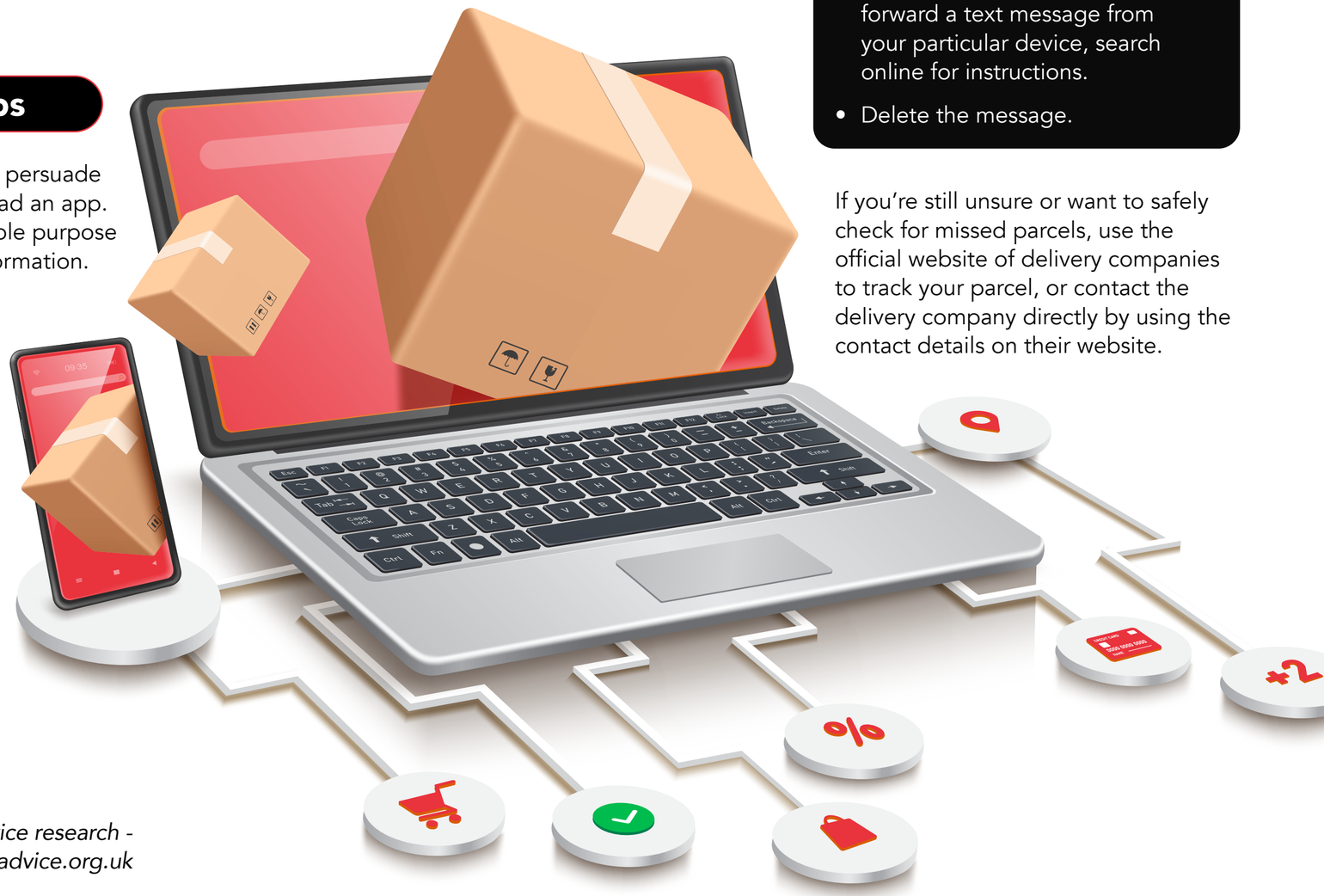
A common way to spot a scam is spelling or grammatical errors – check for mistakes or broken English. Check for United States spelling of words, or obvious incorrect punctuation.

Links and apps

Many delivery scams will often persuade you to click on links or download an app. These are malicious with the sole purpose of obtaining your personal information.

If you receive a message about a missed delivery, even if you're expecting packages, always proceed with great caution and be very suspicious of requests for your personal information.

Most companies will not request a payment via text or email, or request you to download an app, so check on the company's website (don't use the link in the message) to see if this is something they would legitimately do.



Citizens Advice research - www.citizensadvice.org.uk

If you receive a 'missed parcel' message that looks suspicious:

- Do not click the link in the message, and do not install any apps if prompted.
- Forward the message to 7726, a free spam-reporting service provided by phone operators. If you are not sure how to forward a text message from your particular device, search online for instructions.
- Delete the message.

If you're still unsure or want to safely check for missed parcels, use the official website of delivery companies to track your parcel, or contact the delivery company directly by using the contact details on their website.