Delivery Scams

Since the beginning of the pandemic, there has been a huge increase in scam emails and texts related to shipping or deliveries, as more consumers turn to online shopping.

what do delivery scams look like?

Scam texts and emails often appear to have been sent by the Royal Mail or other delivery companies. They could look like the following messages:

- **Your package has a £2.99 unpaid shipping fee.** Pay now by tapping on this link... If not paid a return to sender will be requested.

- **The freight payment for your package was declined.** To get your parcel delivered to your desired destination point you need to pay an extra delivery fee of £1.99. Pay freight.

- **Your Royal Mail parcel is awaiting delivery.** Please confirm the settlement of 1.99 (GBP) using the following link...

- **We’re sorry to let you know that your package which arrived on 25/03/21 will be sent back.** This may happen when the receiver’s address is incorrect. To redeliver please fill out the form: Redeliver my parcel.

- **We attempted to deliver your package at 12:35 on 25/03/21 but nobody was available.** Your parcel was returned to our depot and you need to reschedule your package delivery by pressing here...
how can I tell if a message about a delivery is a scam?

The Royal Mail will never send you an unexpected text message or an email asking for personal or payment details. They 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.

Scam emails often use **impersonal greetings** such as ‘Dear Royal Mail Customer’ and they may contain **spelling and grammatical mistakes**.

Scam delivery messages usually 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.

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

The aim of these messages is to obtain your personal details and payment information. They often ask you to **click on a link**, which will lead to a website with official-looking branding and logos. **Never click on links in unexpected emails or text messages** and never enter any payment or personal details.

If you are unsure whether a message about a delivery is genuine, **contact the company using details found on their official website or in a telephone directory**.

Report all scams to **Advice Direct Scotland** using their free consumer helpline: **0808 164 6000** or via their online reporting tool at **www.scamwatch.scot**.

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](http://www.consumeradvice.scot)
**Police Scotland** - [www.scotland.police.uk/keep-safe](http://www.scotland.police.uk/keep-safe)
**Trading Standards Scotland** - [www.tsscot.co.uk/latest-scams](http://www.tsscot.co.uk/latest-scams)
**The National Cyber Security Centre** - [www.ncsc.co.uk](http://www.ncsc.co.uk)