Parcel delivery scam

Police Scotland alert (received Feb 2021)

Criminals are sending out phishing emails, purportedly from well-known delivery companies, which claim that they have been unable to deliver parcels, packages or large letters. These emails may ask the recipient to pay a fee or provide additional details in order to rearrange the delivery.

The recipient are typically tricked into clicking on links to seemingly genuine websites requesting personal and financial information such as their address, date of birth, mobile number or bank details, which are then used to commit fraud. In some cases, victims later receive a call from the criminal pretending to be from their bank's fraud team, trying to persuade them to move their money to a safe account or reveal their pass codes.

You should also be aware of an increased risk of scam phone calls and texts impersonating delivery companies, as well as fake delivery notices posted through letterboxes. Similarly, these will ask for advance payment or for the recipient to provide information that is later used to defraud them.

Remember that criminals will send out phishing emails with links leading to fake websites used to steal personal and financial information. These emails may appear to be from trusted organisations and may use official branding to convince you they're genuine. Always access websites by typing them into the web browser and avoid clicking on links in emails.

Remain vigilant and check delivery notifications very carefully to ensure they are genuine. Emails, texts or cards through your letterbox may look very similar to those that are genuine but may use generic greetings, such as Dear Sir/Madam, or include spelling errors.

Always question claims that you are due goods or services that you haven't ordered or are unaware of, especially if you have to pay any fees upfront. Consider whether you're expecting a delivery from the company named on the card.

If you receive a delivery card through your letterbox which you do not believe is genuine and which asks you to dial a premium rate number, contact the company direct, using a number you know to be genuine.

You can get more information by following the advice of the Take Five to Stop Fraud campaign.

You can report suspected scam texts to your mobile network provider by forwarding them to 7726, and forward any suspicious emails to report@phishing.gov.uk, the National Cyber Security Centre's (NCSC) suspicious email reporting service.

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101. For all emergency calls, dial 999.

This alert was sent out for your information by Police Scotland Safer Communities Cybercrime Harm Prevention Unit - PPCWCyberHarmPrevention@scotland.pnn.police.uk