



Official

DPD Phishing Scam

Published on 17th December 2020
Reference 20201217

FRAUD ALERT

DPD Phishing Scam



DPD Phishing scam

Published on 08/12/2020

Reference 2010001

5,478 reports of DPD phishing emails were made in November 2020, an increase of 655% when compared to the previous month. Action Fraud has also received 166 reports of suspicious DPD text messages between June and November this year, with a total reported losses of £139,000. Reporting volumes and losses are continuing to increase in the run up to Christmas, with a further 35 reports with a reported loss of £103,000 recorded in the first 8 days of December 2020.

Fraudsters are using fake DPD messages to lure victims into a phishing scam. The messages state that the recipient has missed two attempted deliveries of a parcel, and provides instructions on how to arrange another delivery. The links in the messages lead to fraudulent websites that request a payment (£2 - £3) to rearrange the delivery.

If the victim makes this payment, they'll receive a phone call within a few days from someone purporting to be from their bank to inform them about suspicious transactions on their account. They may also receive text messages, purporting to be from their bank, confirming these transactions. The victim is informed that their bank account may be compromised and is instructed to transfer their money to what they believe is an alternative secure account in order to prevent further losses.

In other cases, suspects have gained enough personal details and security information during the phone call with the unsuspecting victim, to enable them to take out a loan in the victim's name. The fraudsters then transfer the loan to an account under their control. Fraudsters are able to use a tactic called 'spoofing' to make the call or text appear genuine by cloning the phone number, or sender ID, used by the bank.

What you need to do

- There is an easy way to check the email or text is safe, only emails sent from one of three DPD email addresses are genuine. These are dpd.co.uk, dpdlocal.co.uk or dpdgroup.co.uk.
- Your bank, or other official organisations, will never ask you to share personal or financial information over the phone, or via text or email. If you need to check that it's a genuine message, contact them directly.
- If you have received an email which you're unsure about, you can report it by forwarding it to report@phishing.gov.uk. You can report suspicious text messages by forwarding them to **7726**.
- If you have acted upon a message you have received, and you think you may be a victim of a fraud, contact your bank immediately and report it to Action Fraud online at [actionfraud.police.uk](https://www.actionfraud.police.uk) or by calling 0300 123 2040.

For more information about how to protect yourself online, visit
www.cyberaware.gov.uk and takefive-stopfraud.org.uk

Every Report Matters

If you have been a victim of fraud or cyber crime, report it to us at [Actionfraud.police.uk](https://www.actionfraud.police.uk), or by calling 0300 123 2040.