GUIDANCE

FluBot: Guidance for 'package delivery' text message scam

The 'FluBot' spyware, sent via 'package delivery' text messages, affects Android phones and devices

The NCSC is aware that a malicious piece of spyware – known as FluBot – is affecting Android phones and devices across the UK.

The spyware is installed when a victim receives a text message, asking them to install a tracking app due to a 'missed package delivery'. The tracking app is in fact spyware that steals passwords and other sensitive data. It will also access contact details and send out additional text messages – further spreading the spyware.

The text message requests that victims click a link. Doing so directs them to a scam website, such as the one shown below (although the branding may vary).

- Users of **Android** devices (such as those manufactured by Google, Huawei and Samsung) will be encouraged to download an app.
- Users of **Apple** devices are not currently at risk, although the scam text messages may still redirect them to a scam website which may to steal your personal information.

If you receive a scam text message:

1. Do **not** click the link in the message, and do not install any apps if prompted.
2. Forward the message to **7726**, a free spam-reporting service provided by phone operators.
3. Delete the message.

If you were expecting a DHL delivery, you should visit the official DHL website (track.dhlparcel.co.uk) to track your delivery. Do **not** use the link in the scam text message.

If you have already clicked the link to download the application:

You must take the following steps to clean your device, as your passwords and online accounts are now at risk from hackers.

- Do **not** enter your password, or log into any accounts until you have followed the below steps.
- To clean your device, you should:

- Perform a factory reset as soon as possible. The process for doing this will vary based on the device manufacturer and guidance can be found here. Note that if you don't have backups enabled, **you will lose data**.

- When you set up the device after the reset, it may ask you if you want to restore from a backup. You should avoid restoring from any backups created **after** you downloaded the app, **as they will also be infected**.

- To protect your accounts:

- If you have logged in to any accounts or apps using a password since downloading the app, that account password needs to be changed.

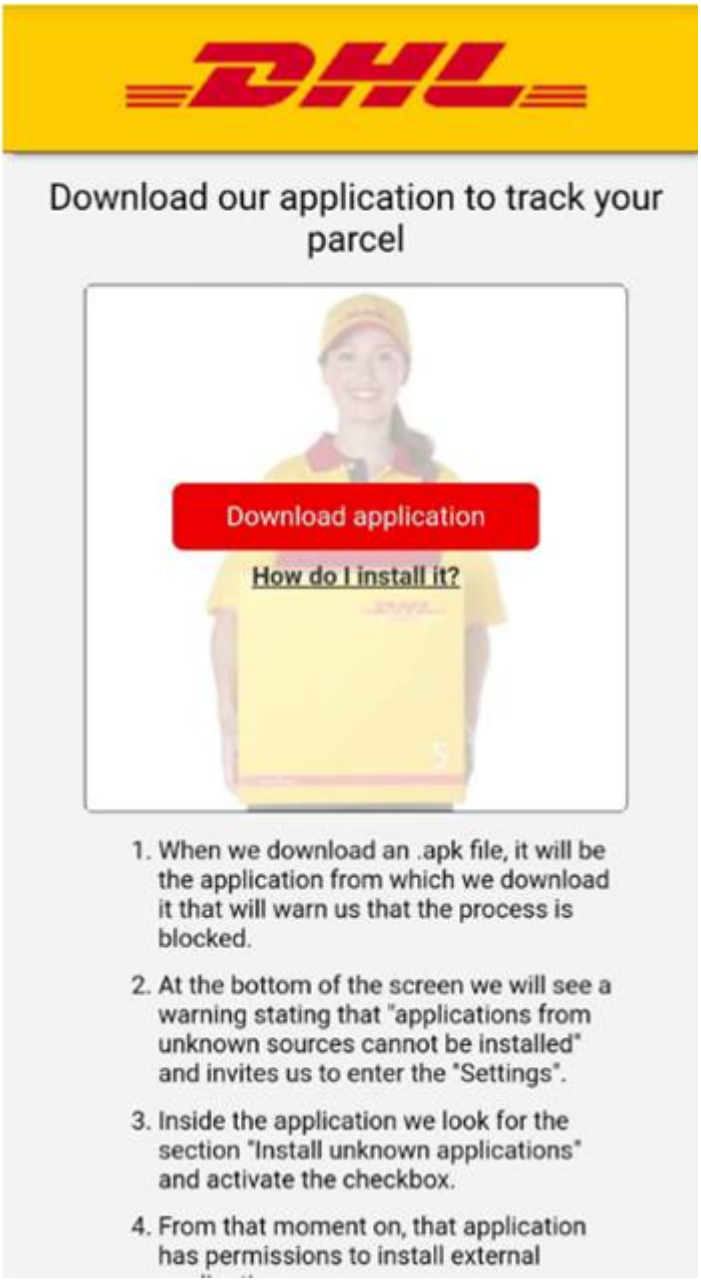
- If you have used these same passwords for any other accounts, then these also need to be changed.

To protect yourself from future scams like this, you should:

1. Back up your device to ensure you don't lose important information like photos and documents. The CyberAware campaign explains how to do this.
2. Only install new apps onto your device from the app store that your manufacturer recommends. For example, most Android devices use Google's Play Store. Some manufacturers, such as Huawei, provide their own app store.

3. For Android devices, make sure that Google's Play Protect service is enabled if your device supports it. Some Huawei devices provide a similar tool to scan devices for viruses. This will ensure that any malware on your device can be detected and removed.

Footnote - While messages so far have claimed to be from DHL, the scam could change to abuse other company brands.



PUBLISHED

23 April 2021

.

REVIEWED

23 April 2021

VERSION

1.0

WRITTEN FOR

Individuals & families

Small & medium sized organisations

Public sector

Self employed & sole traders

Large organisations

Cyber security professionals

Was this article helpful?

Yes No