Cyber Alert - FluBot "package delivery" scam targeting Android devices

The National Cyber Security Centre (NCSC) are advising users of Android phones and devices that a malicious piece of spyware sent via fake package delivery text messages 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.

- Users of Android devices 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 their 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 parcel delivery, you should visit the official website of the courier company or the retailer to track your delivery. Do not use the link in the scam text message.

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.

If you have already clicked the link to download the application to your device or for more information on this scam please visit the following guidance from NCSC.

You can report suspicious emails by forwarding the original message to the Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk

If you receive a suspicious text you can forward this to 7726 which spells SPAM on your phone keypad.

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
Cybercrime Harm Prevention Unit - PPCWCyberHarmPrevention@scotland.pnn.police.uk
All information was correct at time of distribution. 28/04/2021