Be Fraud Smart!
essex.police.uk/befraudsmart
ESSEX POLICE
Protecting and serving Essex

Essex Police Fraud Alert System

34

30th April 2021

FLUBOT—ANDROID USERS BEWARE

Guidance has been issued but the National Cyber Security Centre (NCSC) about 'FluBot' - spyware affecting Android phones and devices that is delivered via the package delivery messages covered by a previous alert.

The spyware is installed when the text message asks them to install a tracking app due to a missed package delivery (currently these scams claim to be DHL but the brand could change). The app is the spyware and will steal passwords and other sensitive data, as well as accessing contacts to send out more text messages.

<u>If you have already clicked the link to download the application:</u>

- 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 via the NCSC website. 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 and if you have used these same passwords for any other accounts, then these also need to be changed.

If you or someone you know is vulnerable and has been a victim of fraud, please call **Essex Police** on **101**
Report fraud or attempted fraud by contacting **Action Fraud** at **actionfraud.police.uk** or call **0300 123 2040**

Keep up to date with fraud and do *even more* Online at **essex.police.uk**

CALL ESSEX POLICE 101
IN AN EMERGENCY ALWAYS CALL 999

Essex Police Fraud Alert System

ESSEX POLICE
Protecting and serving Essex

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** (spells SPAM on your keypad), a free 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.

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. Search for the **CyberAware** campaign which 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.

TAKE FIVE

TO STOP FRAUD™

STOP. CHALLENGE. PROTECT.

If you or someone you know is vulnerable and has been a victim of fraud, please call **Essex Police** on **101**
Report fraud or attempted fraud by contacting **Action Fraud** at **actionfraud.police.uk** or call **0300 123 2040**

CALL ESSEX POLICE 101
IN AN EMERGENCY ALWAYS CALL 999

Keep up to date with fraud and do *even more* Online at essex.police.uk