Look out for Android “police” malware

The National Fraud Intelligence Bureau has issued some advice on how to remove Android-Trojan.Koler.A Malware that displays a warning message which appears to come from the police [30 May 2014]

You will know your device is infected when a pop appears on your screen displaying a warning message, which claims to come from the police or other crime agencies.

The pop up states that your device been locked, and can be unlocked if you pay a fine. This type of malware is designed to prevent you from accessing your home screen as well as other apps on your Android device. The malware achieves this by disabling the back space button.

How does if get infected?

This type of malware can only infect your device if you install it, usually through the download of a new application.

One method seen is being asked to download new video software to view premium videos. Once accepted the Trojan launches a browser, which briefly displays the logo of the app it is impersonating. Whilst the download is occurring, the Trojan accesses the phones Geolocation to establish the country you live in, it also takes note of your IMEI number.

How to remove the malware?

This type of malware can be removed from your phone and it is recommended that you don’t pay to remove the warning message, as it is unlikely to resolve the issue.

Two methods:

1. Although the back space button is disabled there is a limited period (5secs) given to access the home screen where the app can be uninstalled. This is done by pressing the home screen button, navigating to the app, then dragging it to the top of the screen where the uninstall control is located.

2. Removal can also take place by booting the device in safe mode and then uninstalling the app.

Not all Android devices will have the same method to enable safe mode, it is recommended that you check how to do this based on your device make and model.

Although the malware can be removed, fraudsters will still have gained your IMEI number. IMEI is a 15 or 17 digit unique number to identify mobile devices, as well as some other devices. It is usually found printed on the phones back under the battery.

If you think you have been a victim of this type of fraud you should report it to Action Fraud 0300 123 2040, the UK’s national fraud reporting centre. Please state the device being used, the website and the application downloaded