Flubot

You may have recently received a letter and/or email from Sunrise explaining that we have been notified a device on your network has been infected by malware named Flubot. If you have received such a communication from us, please follow the advice given on this page to resolve the issue.

Overview

Flubot is a type of malware mainly affecting Android devices, it is distributed via SMS messages that notify a user of a 'missed package delivery' or 'voicemail' which provides a link to an app – this is in fact a tracking app designed to steals passwords and sensitive data. Once on a user's device it will also access contact details and distribute further messages.

Apple users can still be affected as the text messages will direct them to a site that can take their personal information.

What has happened?

We work with several not-for-profit organizations that collate information on devices across the Internet that are infected with malware. They have notified us that a device on your home Internet connection (or one connected to your home network) is infected with malware.

We are unable to specify exactly what device in your home is infected, but it is highly likely to be an Android device as this type of malware targets users through an Android app via a text message link.

If the malware is not removed, the device can be exploited to unwittingly participate in malicious activities.

It is therefore important that you follow the advice in this article.

Note: This article is intended to provide advice. Sunrise is not responsible for any issues encountered in the course of resolving the issue and is not able to provide any technical support for such problems.

How can the issue be fixed?

If you receive the text message, please ensure to complete the following:

- Do not click the link and do not install any apps, if requested.
- Forward the message to 7726 – this is a free spam reporting service supported by most phone operators
- And finally, delete the message

If you have clicked the link in the text message and downloaded the app you will need to perform a full factory reset on your device to ensure the malware is removed, please refer to your manufacturers guide for assistance with performing a factory reset. Before this is done please ensure not to login to any accounts on the device. If you have logged into an account on or after the date you have been infected, we strongly advise you change the password for that account.

Be aware that if you do not have backups enabled, you will lose data.

How do I know I'm now safe?

If you have followed the above advice you can be confident that you have resolved the issue.

Internet Matters

Sunrise is a Co-Founder and Member of iBarry.ch: a not-for-profit organisation working with online safety experts to bring you all the information you need to help keep you and your children safe online.

For more information about iBarry, please visit https://www.ibarry.ch