



IT Security & Mobility Solutions

www.avr.co.uk +44 (0)1189 344 300



How to know if you've been impacted by Pegasus

What to do about it

The guidance below will help you determine if you are impacted by the Pegasus threat. Pegasus is a sophisticated attack that uses three vulnerabilities in the iOS software, collectively known as Trident, that, when exploited, enables attackers to install spyware on your device.

Note: Lookout believes the vast majority of users will not be impacted by Pegasus given the sophisticated, targeted nature of the attack.

If you are an individual looking to protect your personal device, please follow the guidance outlined in the **Lookout Personal** section below.

If you are an employee of a company or have IT / Infosecurity responsibilities at your organization and are looking to protect corporate mobile devices, please follow the guidance outlined in the **Lookout Mobile Endpoint Security** section below.

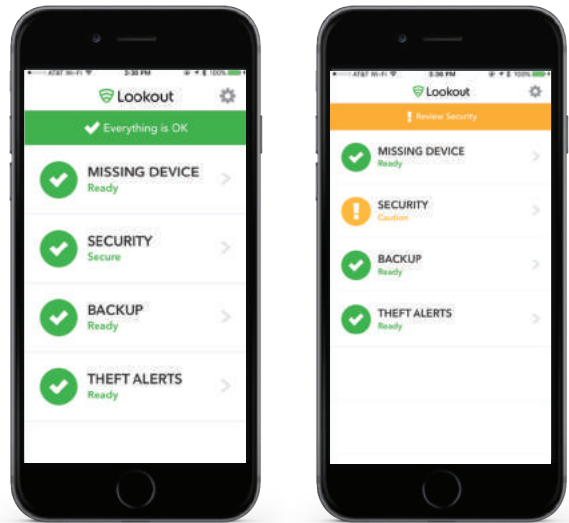
Lookout Personal

To start, if you do not yet have Lookout, you can download the Lookout app from the [Apple App Store](#) and then create an account with your email address and a password of your choosing.

STEP 1: Update your iOS operating system immediately to 9.3.5, which includes a recently released fix from Apple. Go to Settings, tap 'General', then 'Software Update', and then 'Install Now'.

STEP 2: Update to the latest version of Lookout (4.4.8) from the Apple App Store. Open the App Store on your device, search for Lookout, then tap 'Update'.

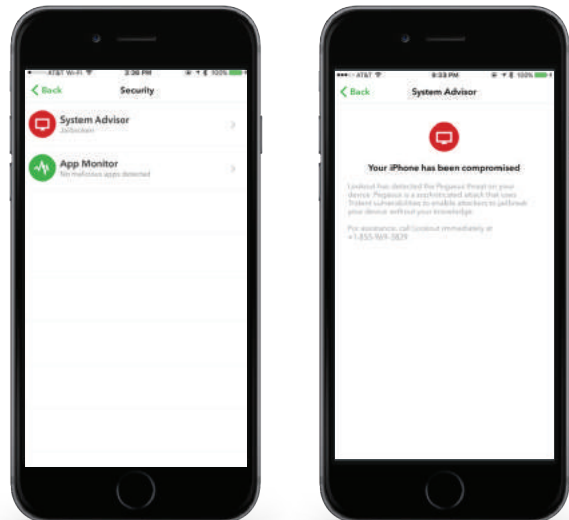
STEP 3: Open the Lookout app on your device. Confirm that your Lookout dashboard shows a green "check" in the Security section, indicating that Everything is OK. If you see a yellow "exclamation mark" instead, tap on "Security".



STEP 3

STEP 4: On the next screen tap "System Advisor"

STEP 5: You will be taken to the "System Advisor" description screen. If your device is impacted by the Pegasus threat, you will see the following screen and message.



STEP 4

STEP 5

Lookout Mobile Endpoint Security

If your organization does not currently have Lookout Mobile Endpoint Security, please [contact us](#) for assistance. If your organization already has purchased Lookout Mobile Endpoint Security, see below for guidance:

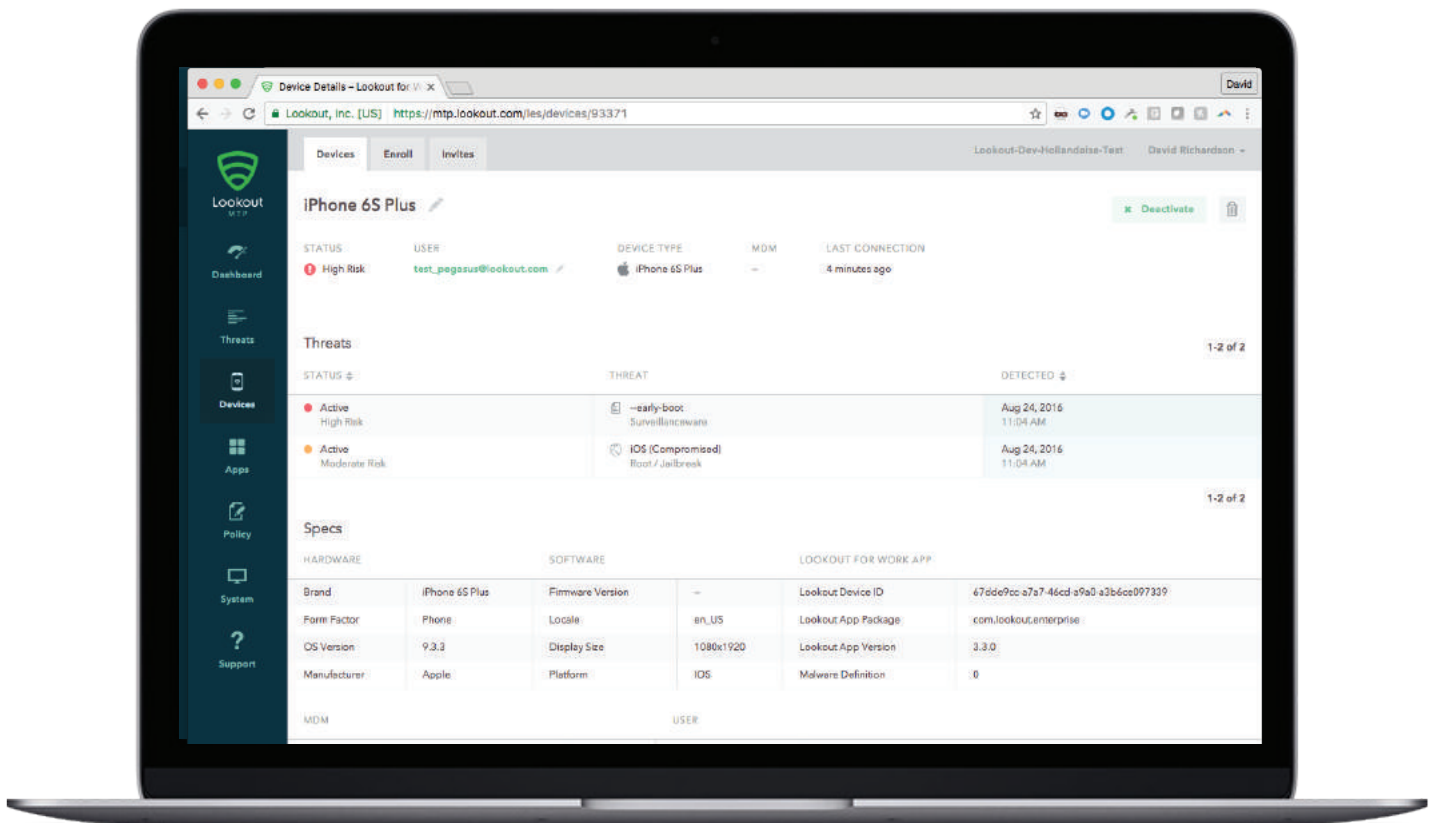
STEP 1: Ensure all of your employees' devices are updated to the latest iOS operating system version - iOS 9.3.5

STEP 2: Determine if your employees' devices have been impacted by the Pegasus threat.

Lookout can detect the Pegasus threat on devices where the Lookout app is **deployed and activated**.

Administrator Notification

If the Pegasus threat is identified on one of your devices, you will see the following threat notifications in the [Lookout admin console](#):



Note: Lookout detects /--early-boot as Surveillanceware named Pegasus

End User Alerts

