



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

Advanced Cyber Security (ACS)

Lab – Hacking Mobile Platform

**Faculty of Architecture, Computing &
Engineering
School of Applied Computing
IQ Building, Room 205
Swansea
SA1 8EW**

A mobile device allows communication between users on radio frequencies. It can also be used to send multimedia content, email, and do much more using the Internet.

Task 1: Securing Android Devices from Malicious Applications

Sophos Mobile Security app provides full functionality to protect your Android device. Using up-to-the-minute intelligence from SophosLabs, you can scan your apps on demand or at the interval of your choice.

Lab Scenario

Android's growing popularity has led to increased security threats, ranging from common malware to advanced phishing and ID theft techniques. To help Android users to deal with these issues, many security software companies have launched their own security apps, but paying nearly 30 dollars a year for a complete mobile security app doesn't sound like a good deal, especially when there's a wide choice of free security apps that will cover all your needs including a group of complete security suites with anti-theft capabilities.

The penetration tester will scan for any unsecure settings your device may have and will advise you accordingly. The Privacy Advisor, on the other hand, scans and lists all the installed apps and categorizes them under three categories: apps that may cause costs, apps that may harm your privacy and apps that may access the Internet. You can sort the categories to your own needs using the icons at the bottom. The Spam Protection is a very simple yet effective call and SMS filter, and the recently added App Protection will lock any app you want with an alphanumeric password.

Lab Objectives

The objective of this lab is to help students learn to:

- How to scan for malicious applications and files on Android mobile devices
- How to uninstall malicious applications
- How to delete the malicious files
- How to secure your mobile device from unknown sources apps

Pre- Activity exercise

To carry out the lab, you need:

- A computer running Windows
- Android emulator running in virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Overview of Lab

Sophos Mobile Security automatically scans apps as you install them. This anti-virus functionality helps you to avoid undesirable software which can lead to data loss and unexpected costs. It also protects your device from attacks via USSD or other special codes. And if your device is lost or stolen, a remote lock or wipe will shield your personal information from prying eyes.

Activity:

Note: Screenshot may varies from the one in this lab.

1. Launch **Android** Emulator in Hyper-V Manager, and click **Play Store** icon from the Home Screen.
2. Make sure that **google** account has added it in the Play Store; if not, create a new one and add the account.

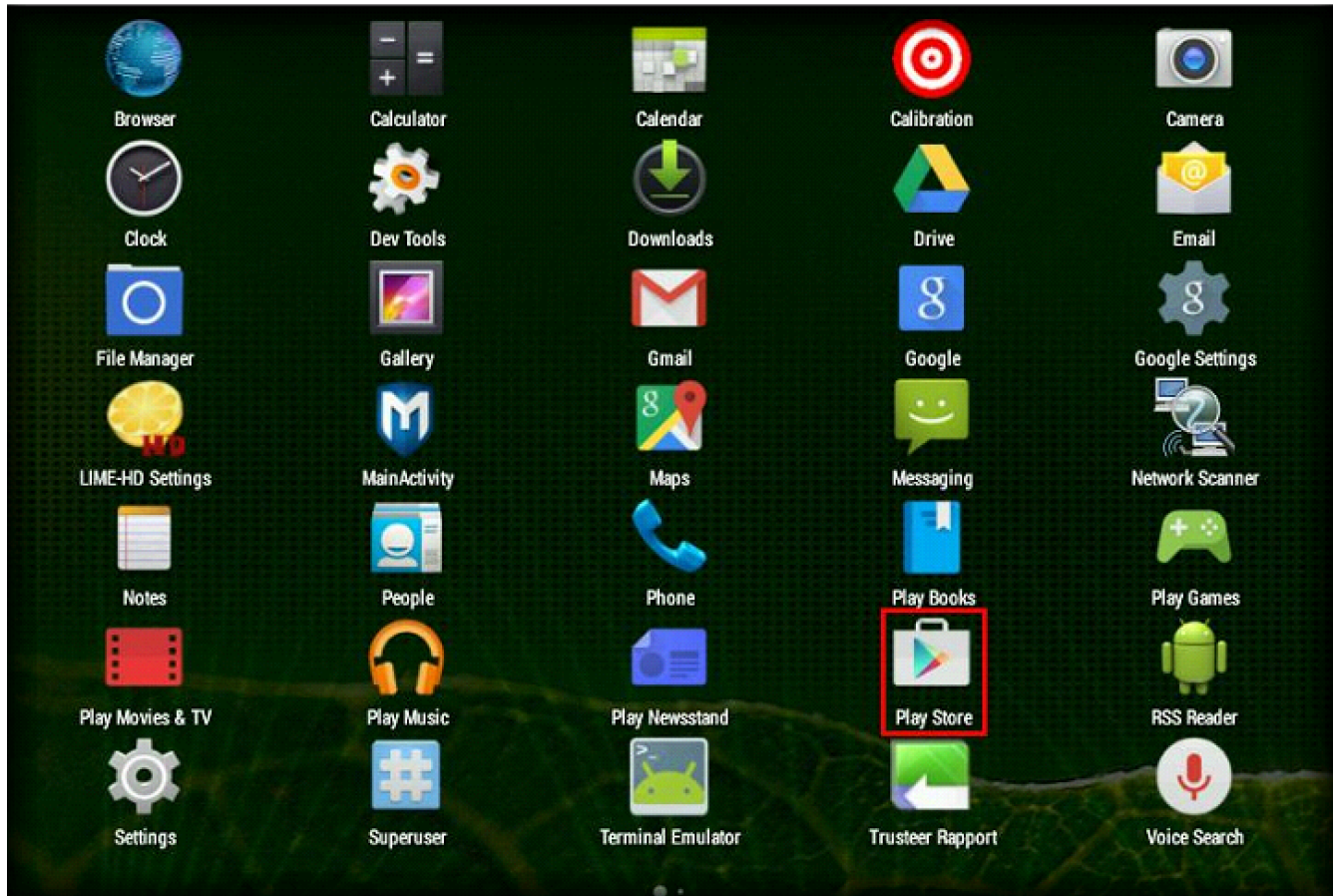


FIGURE 4.1: Android Emulator Launching Play Store

3. In the Play Store bar, type **Sophos Mobile Security** and press **Enter** to display the search results for Sophos applications, as shown in the screenshot.
4. Click **SOPHOS Free Antivirus and Security** app to view application information.

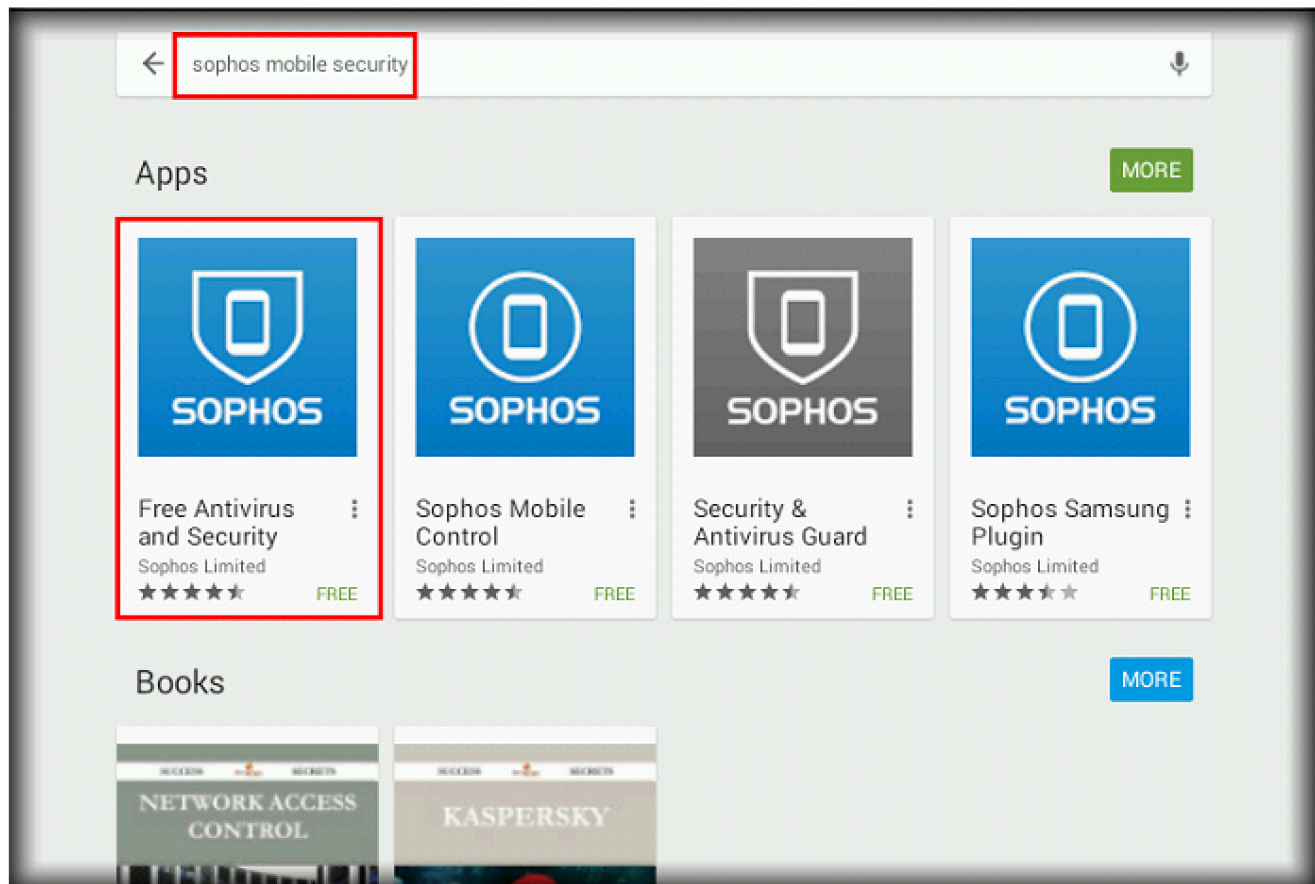


FIGURE 4.2: Searching SOPHOS in Play Store

5. Click **INSTALL** to start installation of SOPHOS Free Antivirus and Security.
6. You can also read further by scrolling down.



FIGURE 4.3: Installing SOPHOS Free Antivirus and Security

7. Sophos Free Antivirus and Security needs to access information. When the pop-up appears, click **ACCEPT**.

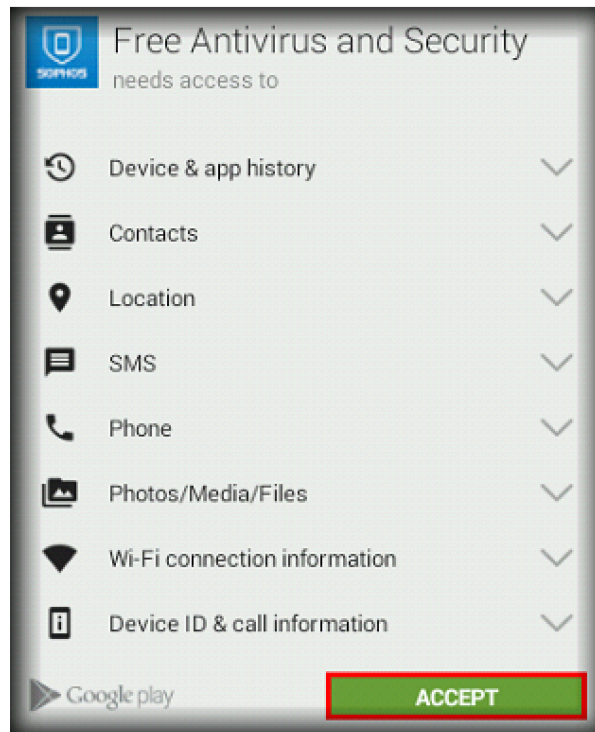


FIGURE 4.4: SOPHOS Notification

8. Sophos Free Antivirus and Security will start downloading, as shown in the screenshot.

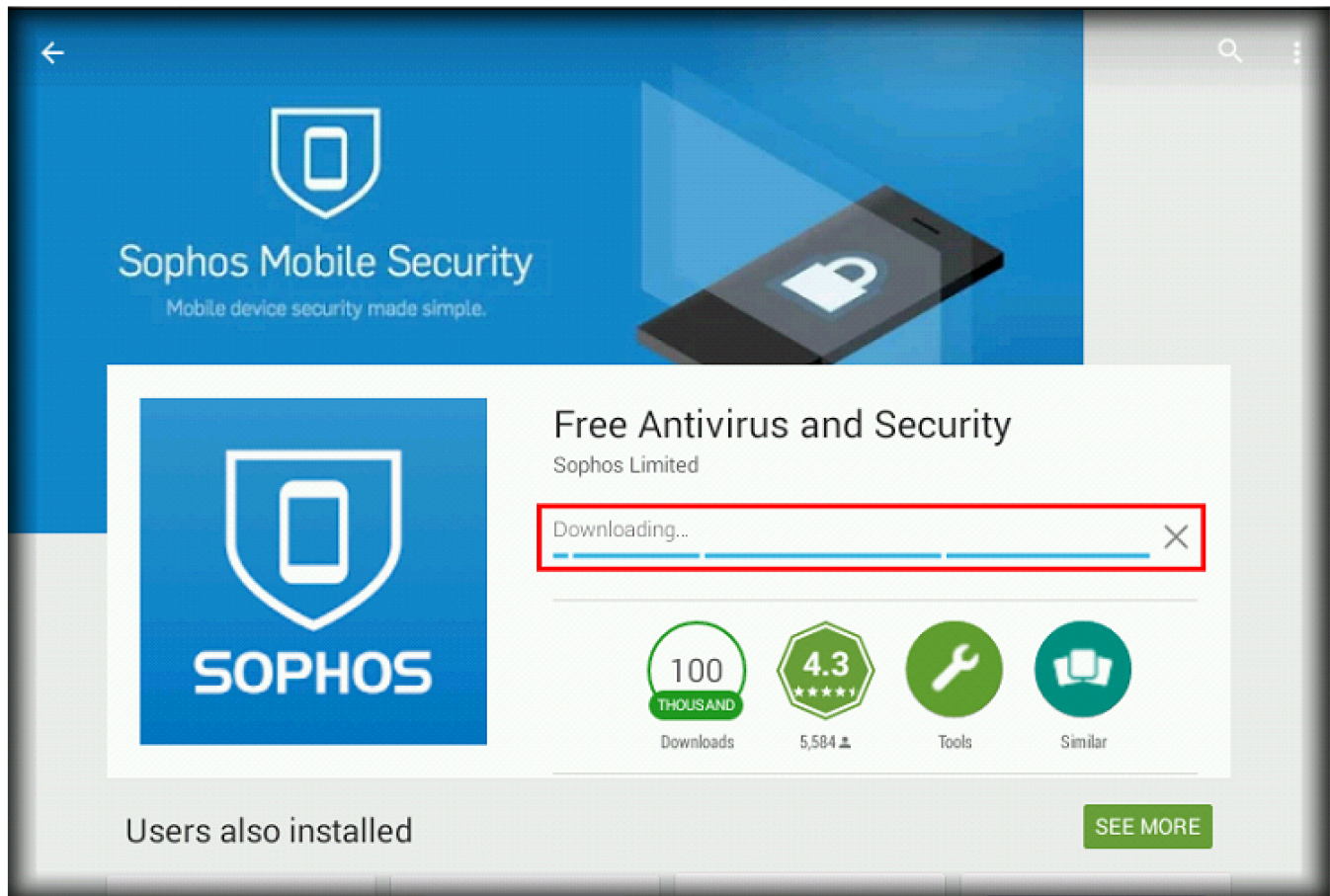


FIGURE 4.5: SOPHOS Downloading required Files

9. Once the application is installed, click **OPEN** to launch it.

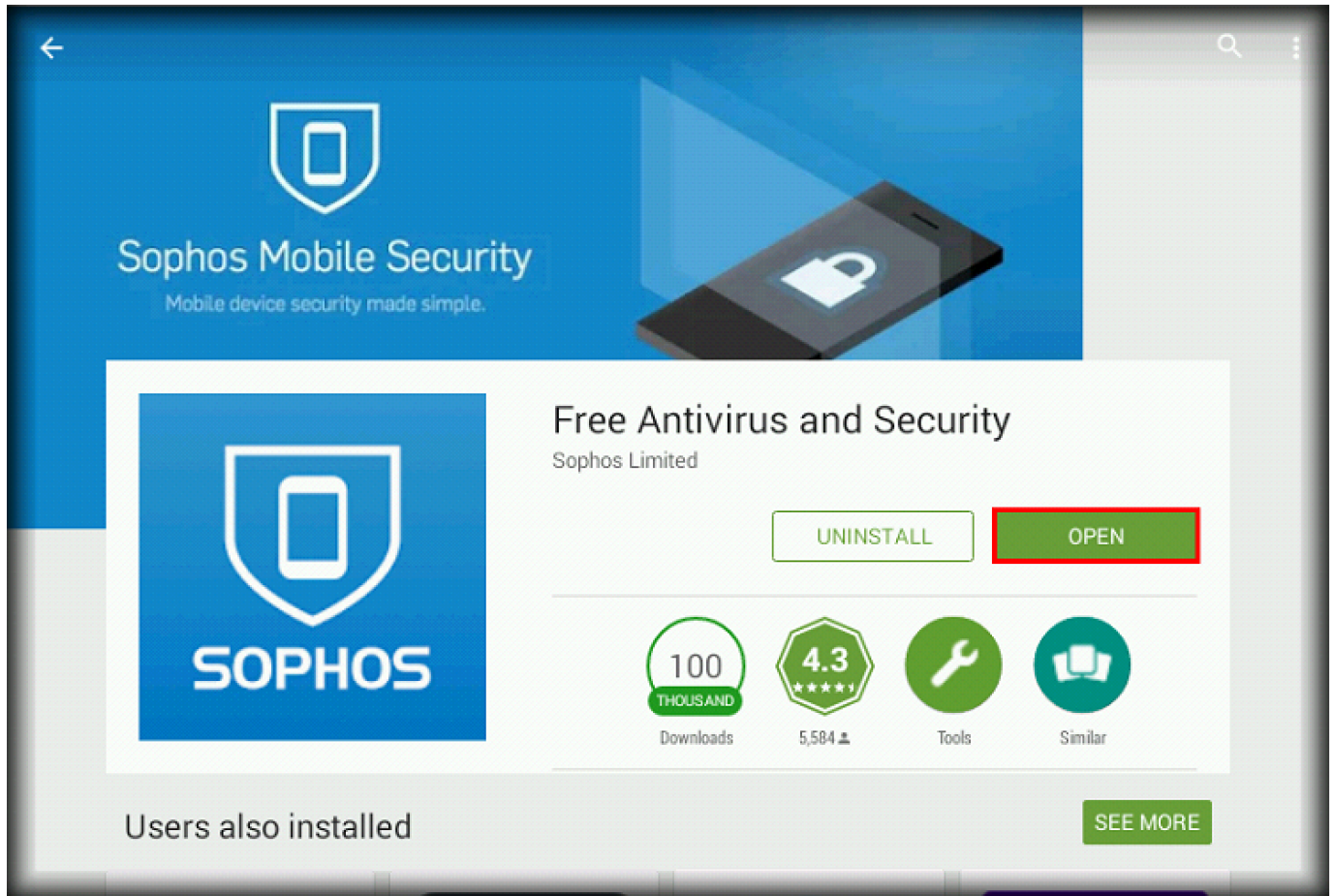


FIGURE 4.6: SOPHOS Application Installed and Launch

10. Once the application is installed, you can also launch it from the **Apps** menu.

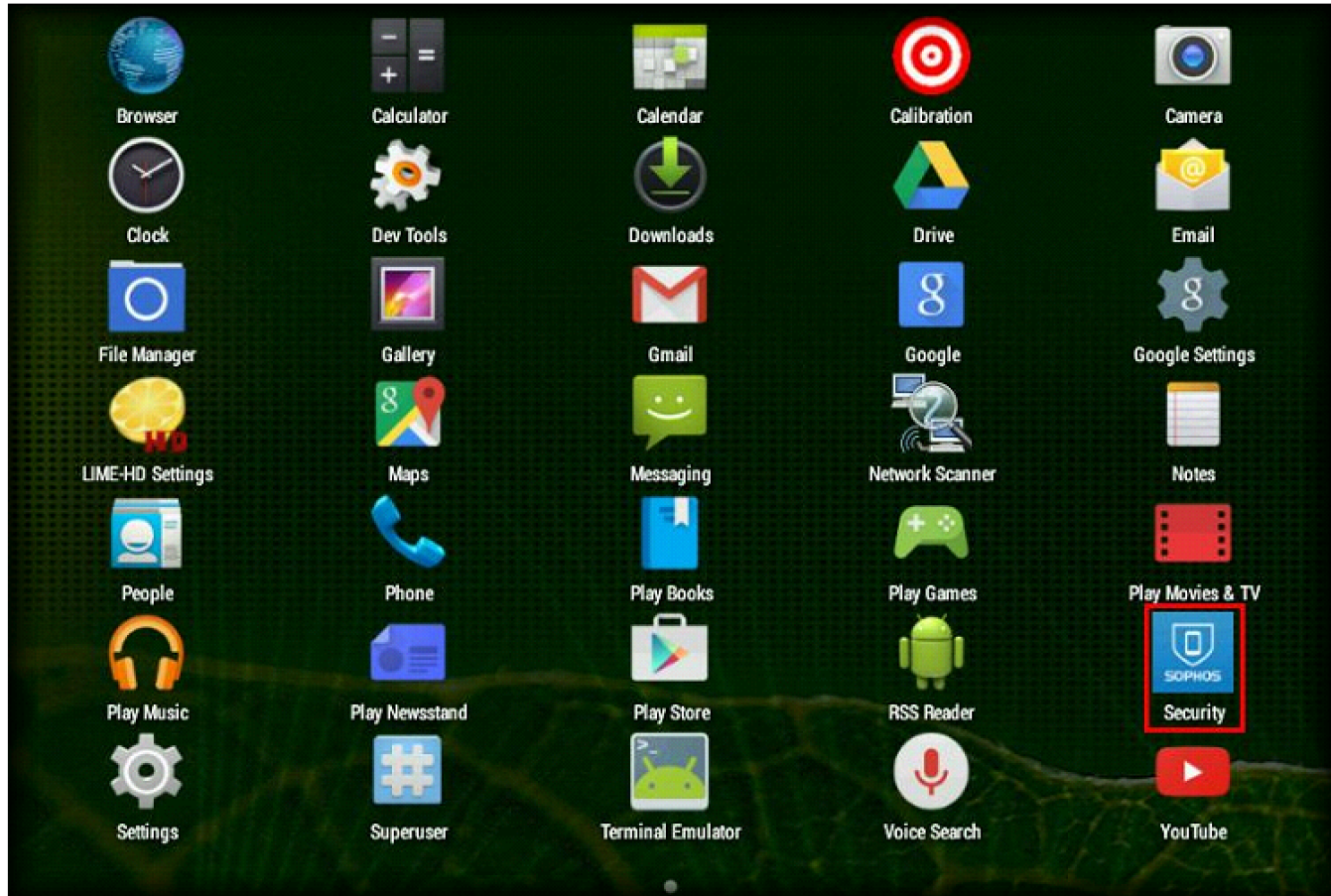


FIGURE 4.7: SOPHOS Alternatively Launch

11. EULA Sophos Mobile Security license agreement will appear. Check **Allow sending anonymous usage information**, if necessary, and click **Accept**.

EULA Sophos Mobile Security 5.0.1515

SOPHOS END USER LICENSE AGREEMENT

Please read the following legally binding License Agreement between Sophos and Licensee carefully. By selecting the accept option, breaking the seal on the software package, or installing, copying or otherwise using the Products, Licensee acknowledges that Licensee has read, understands, and agrees to be bound by the terms and conditions of this License Agreement, including without limitation the terms and conditions of documents and policies which are incorporated herein by reference.

If Licensee does not agree with the terms and conditions of this License Agreement, Licensee is not authorized to install or otherwise use the Products for any purpose whatsoever. If Licensee returns the unused Products and all accompanying items in their original condition and packaging within twenty-one (21) calendar days of delivery by Sophos, together with proof of purchase, Licensee may receive a full refund.

Where a reseller, service provider, consultant, contractor or other party downloads, installs or otherwise uses the Products on Licensee's behalf, such party will be deemed to be Licensee's agent and Licensee will be deemed to have accepted all of the terms and conditions of this License Agreement as if Licensee had directly downloaded, installed or used the Products.

NOW IT IS AGREED as follows:

1. DEFINITIONS

1.1 'Affiliates' means, with respect to each party, entities that control, are controlled by, or are under common control with such party. For the purposes of this definition, "control" means the beneficial ownership of more than fifty per cent (50%) of the voting power or equity in an entity.

1.2 'Computer' means any device or computing environment which benefits from the Licensed Product (for example but without limitation, workstations, personal computers, laptops, netbooks, tablets, smartphones, and environments connected to an email server, an internet proxy or a gateway device, or a database). The Licensed Product does not have to be physically installed on the computer environment to provide benefit, nor is there a requirement for the computing hardware to be owned by the Licensee. The term Computer as defined herein includes, without limitation, non-persistent deployments, electronic devices that are capable of retrieving data, and virtual machines.

1.3 'Documentation' means documentation provided to Licensee by Sophos (whether electronic).

☒ Allow sending anonymous usage information

Decline Accept

FIGURE 4.8: EULA Sophos Mobile Security Agreement

12. Sophos Mobile Security main window appears, as shown in the screenshots with their respective selected options.

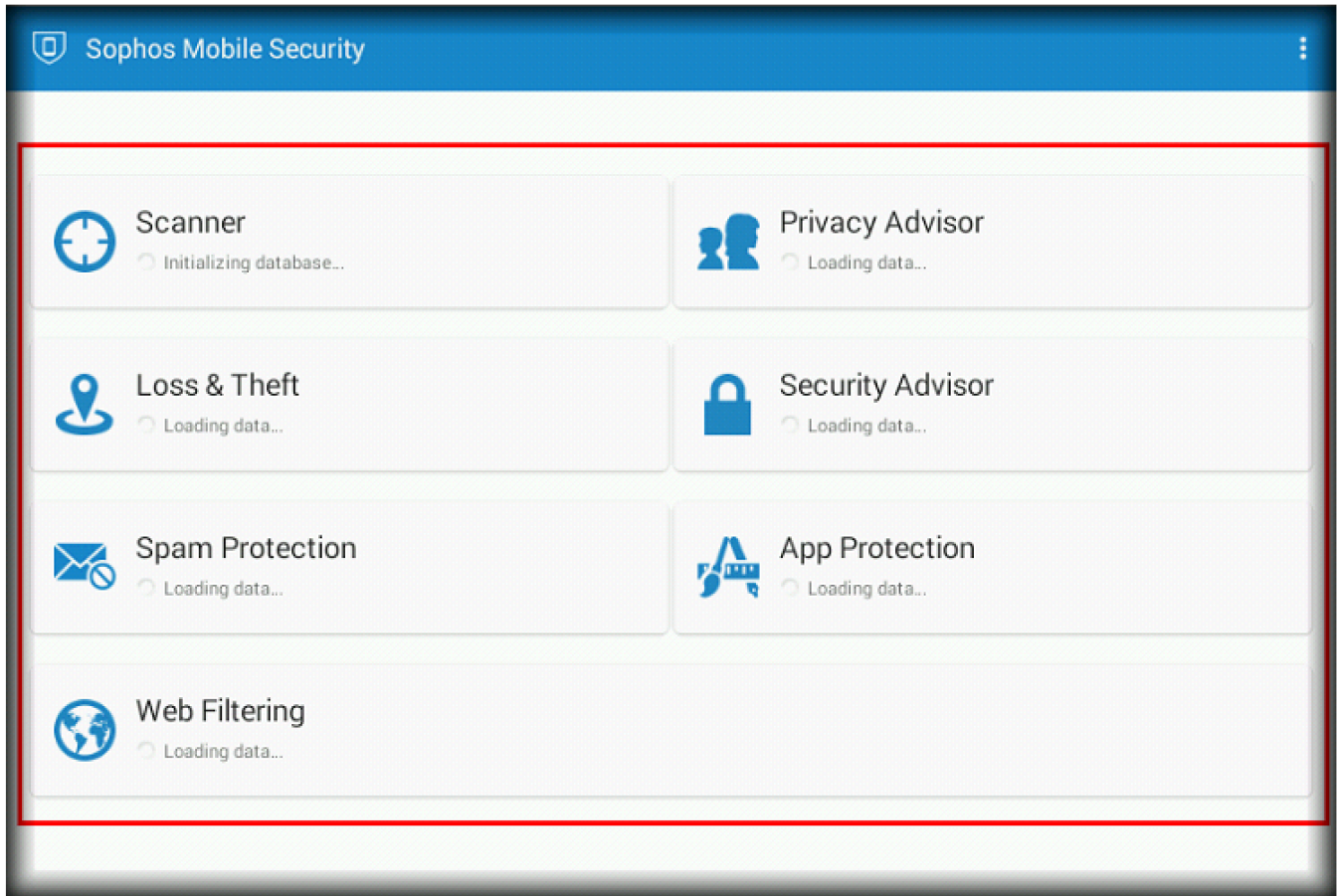


FIGURE 4.9: SOPHOS Mobile Security Main Screen

13. Click **Scanner** to start the scan for malicious applications on your Android device.

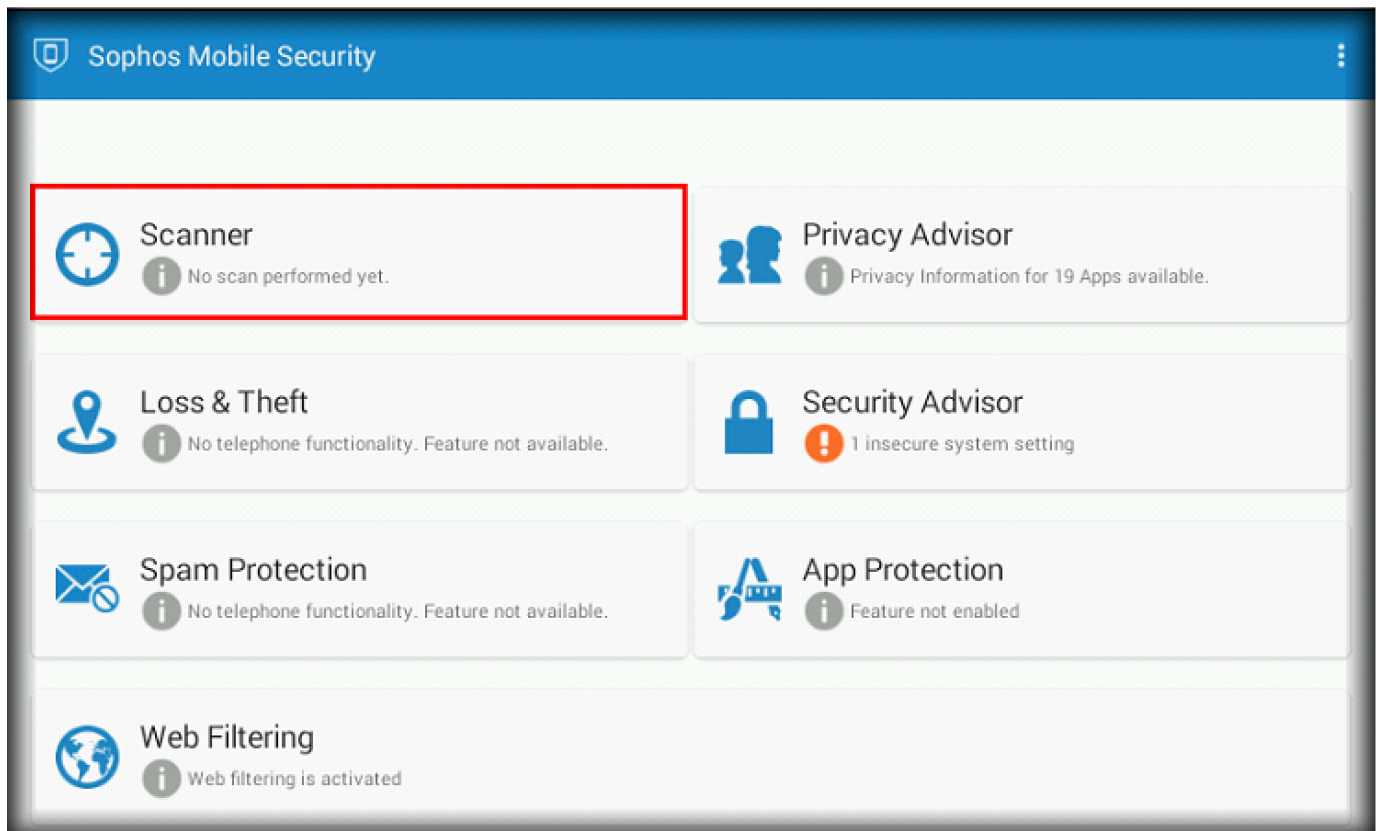


FIGURE 4.10: Sophos Mobile Security Malware Scanner

14. The Sophos Mobile Security Scanner window appears; it is divided into four sections.
15. Click **Start**, under **Malware Scanner**, to start the scan.

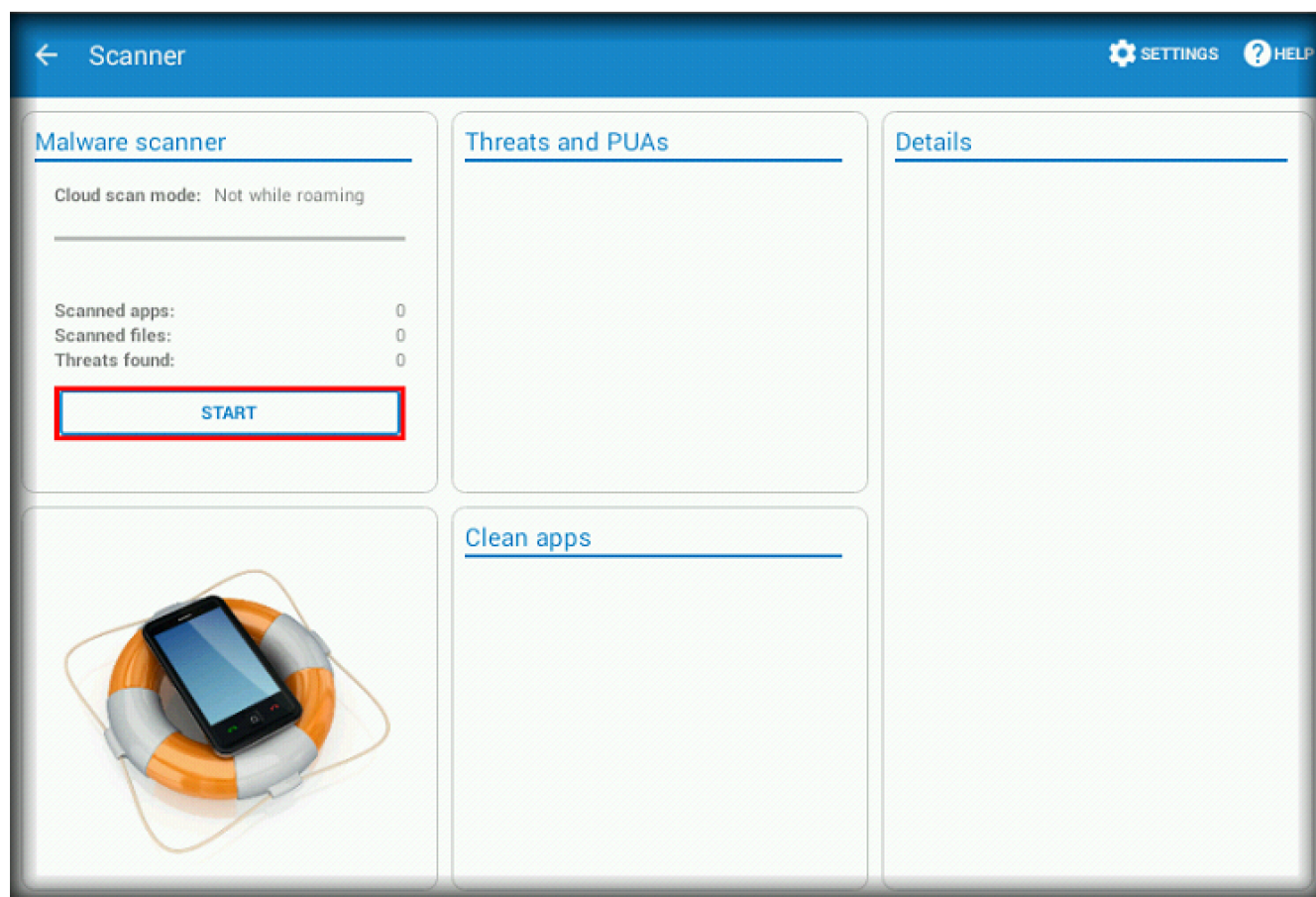


FIGURE 4.11: Sophos Starting Malware Scan

16. Once the scan starts, you can see its status under Malware scanner.

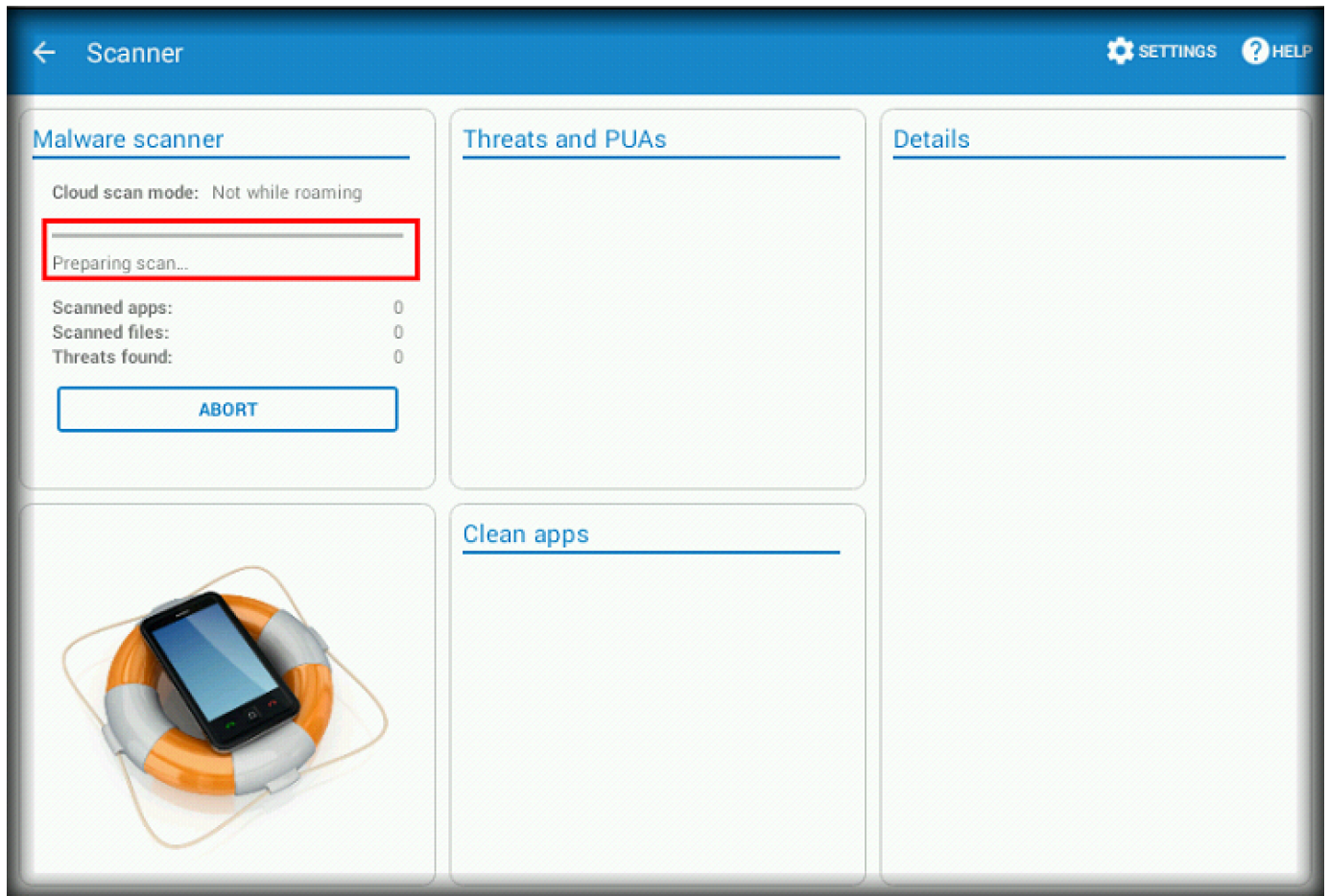


FIGURE 4.12: Sophos Malware Scanner Preparing for Scan

17. Once the scan is complete, it will display the **Scanned apps**, **Scanned files**, and **Threats found** on the mobile device.

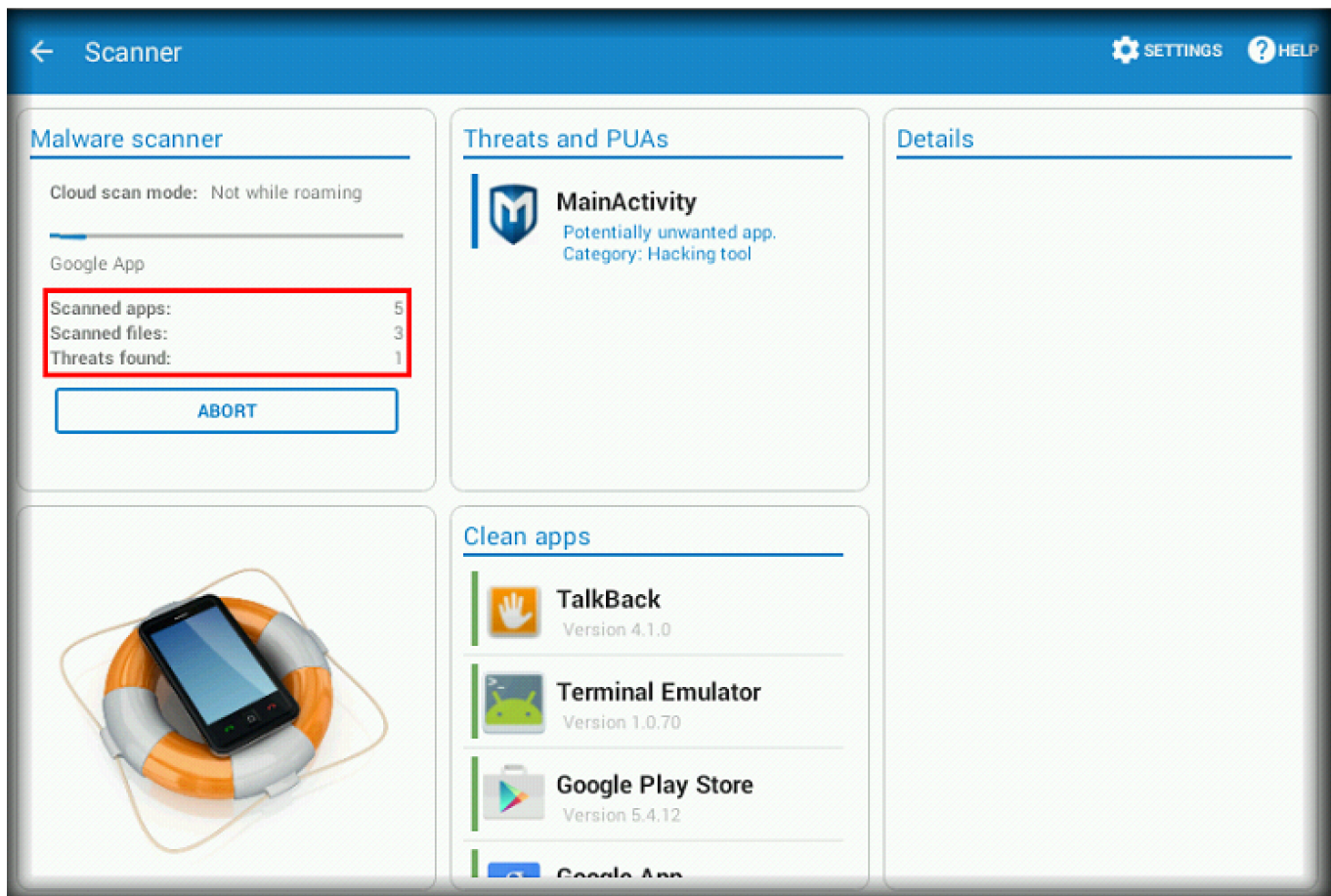


FIGURE 4.13: Sophos Malware Scanning Status

18. The Malware Scanner is complete and displays malicious applications and files under Threats and PUAs, Clean applications under Clean apps, and the Details section displays the information about the application installed on the mobile device.

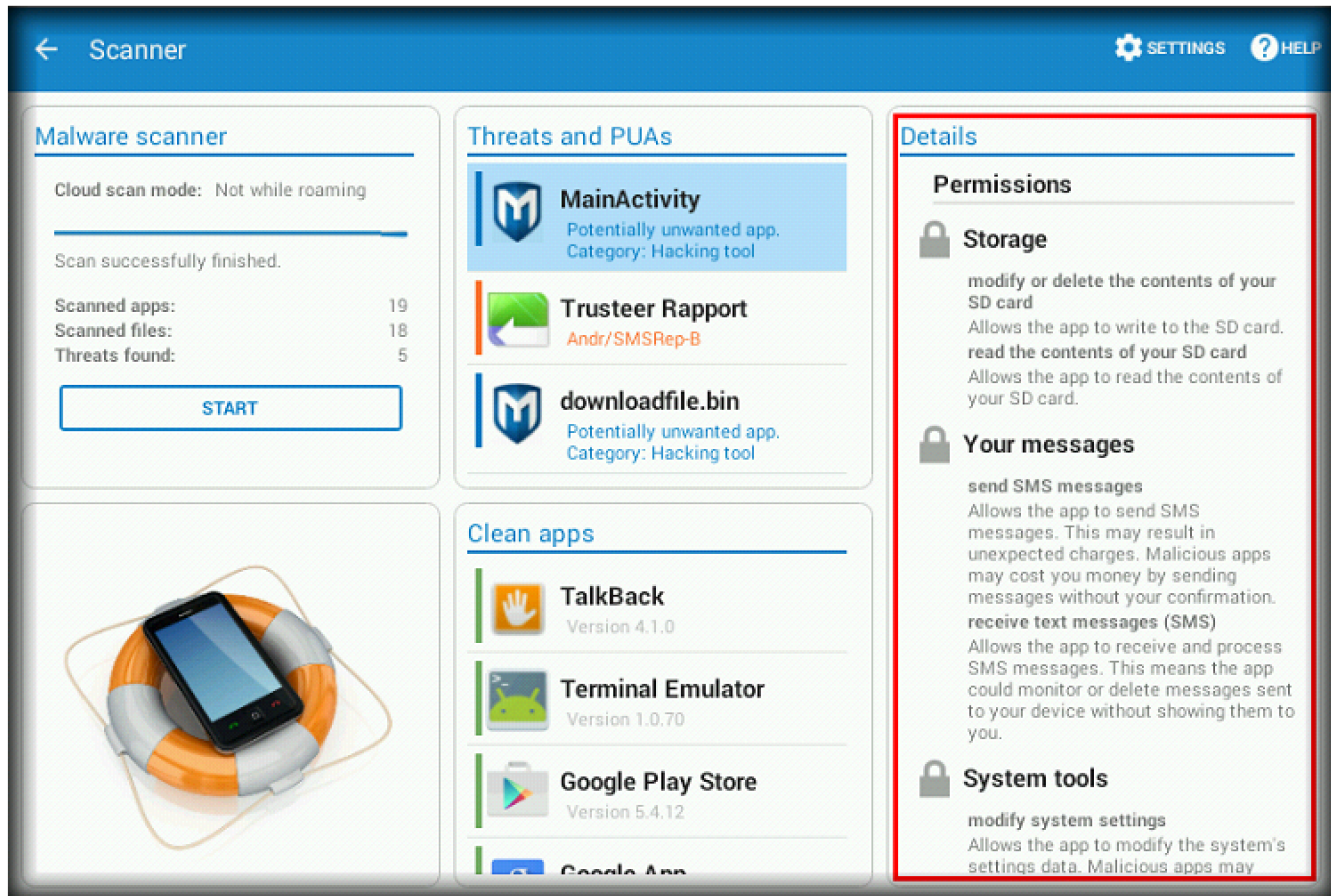


FIGURE 4.14: Sophos Detected Threats Information

19. Now, choose any application under Threats and PUAs, and click **Uninstall** to uninstall the malicious application from the mobile device.

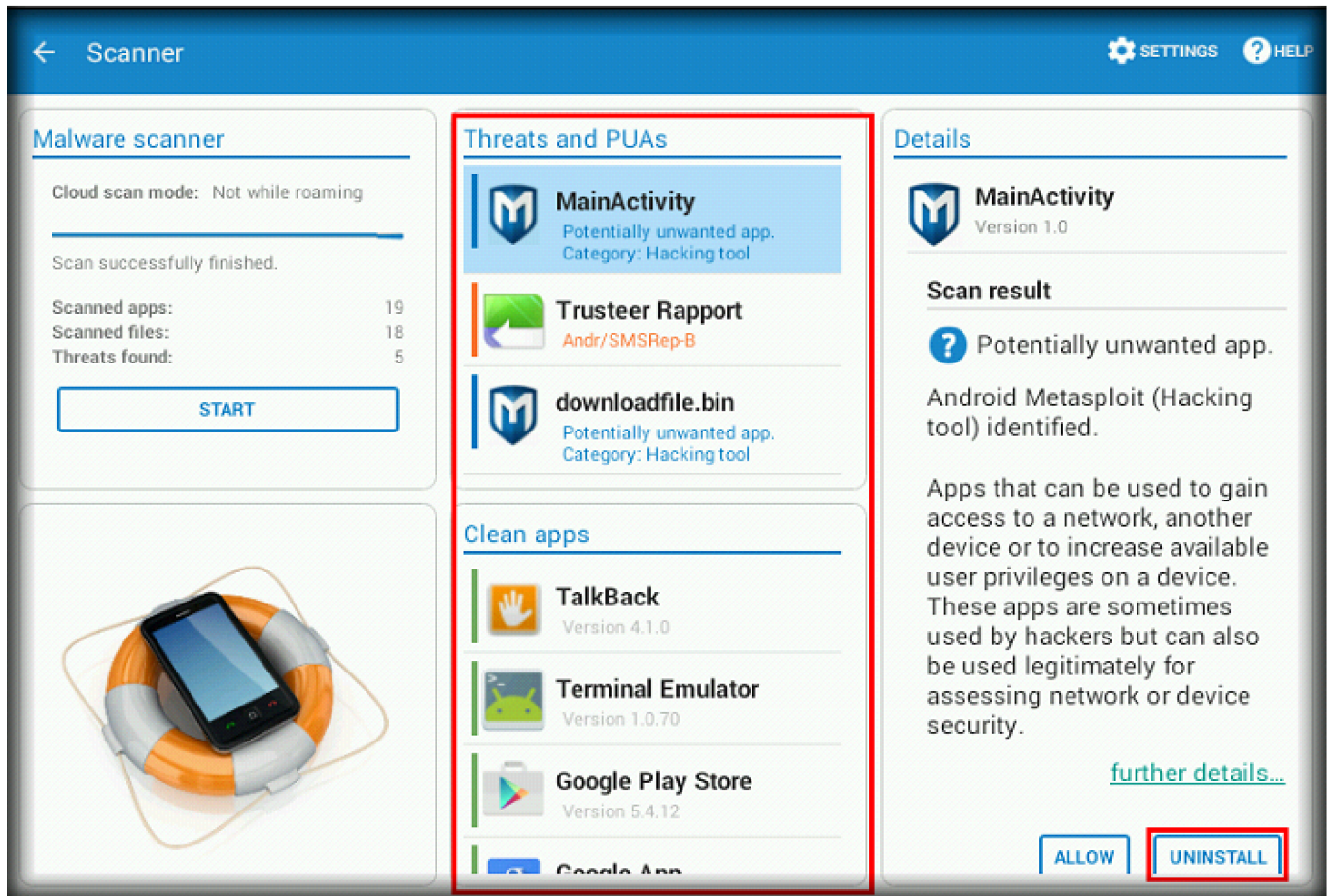


FIGURE 4.15: Sophos Uninstalling Potentially Unwanted Application

20. Similarly, uninstall other applications from the mobile device that have been found to be untrustworthy.

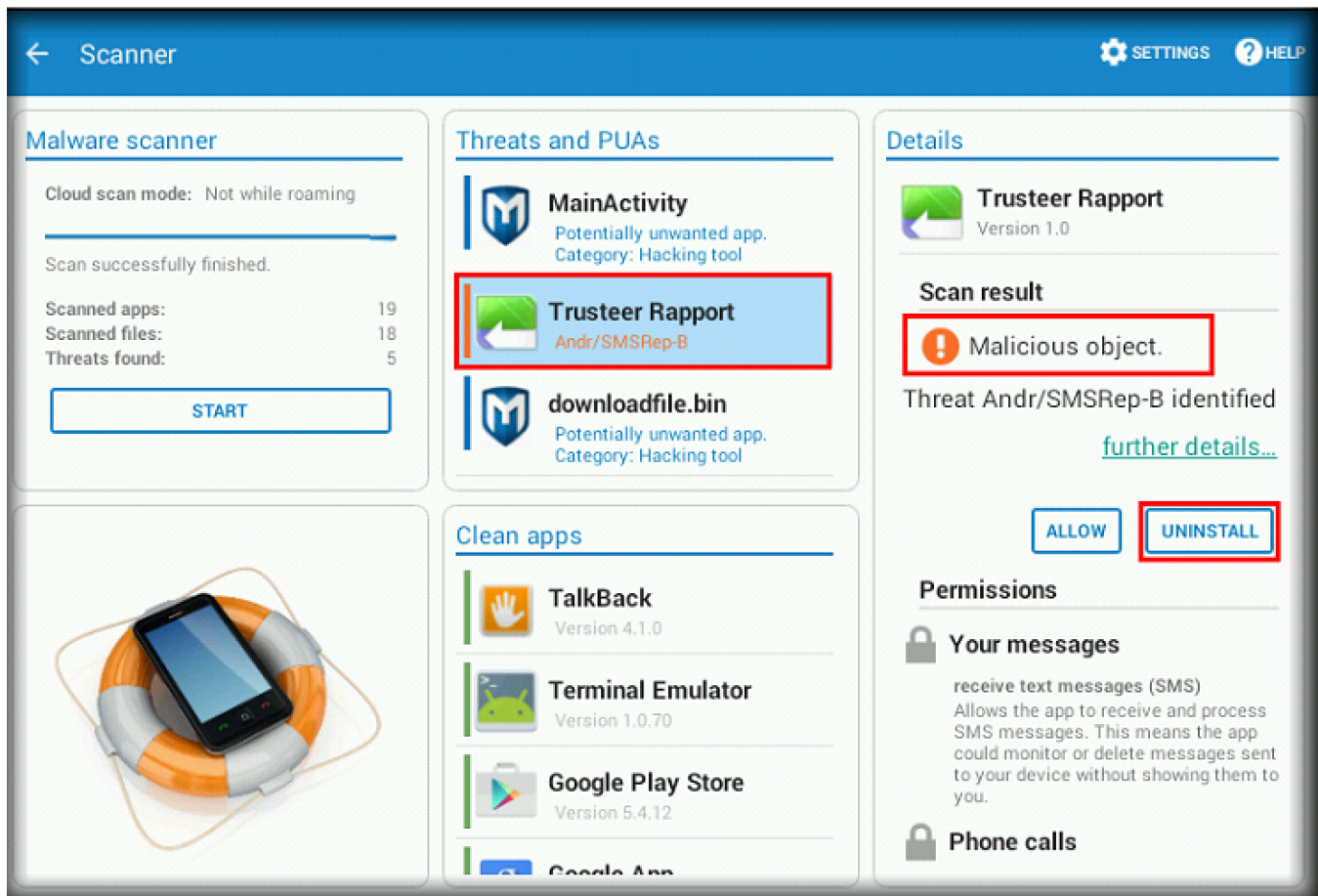


FIGURE 4.16: Sophos found Malicious Object

21. Some applications, while uninstalling, will ask for the permission of the user to do so; click **OK** to confirm.

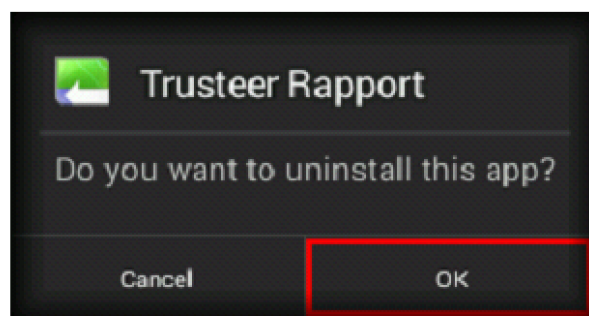


FIGURE 4.17: Confirming Uninstallation of app

22. Choose a malicious file in the Threats and PUAs section, and click **DELETE**. It will delete the malicious file permanently from the mobile device, as shown in the screenshot.

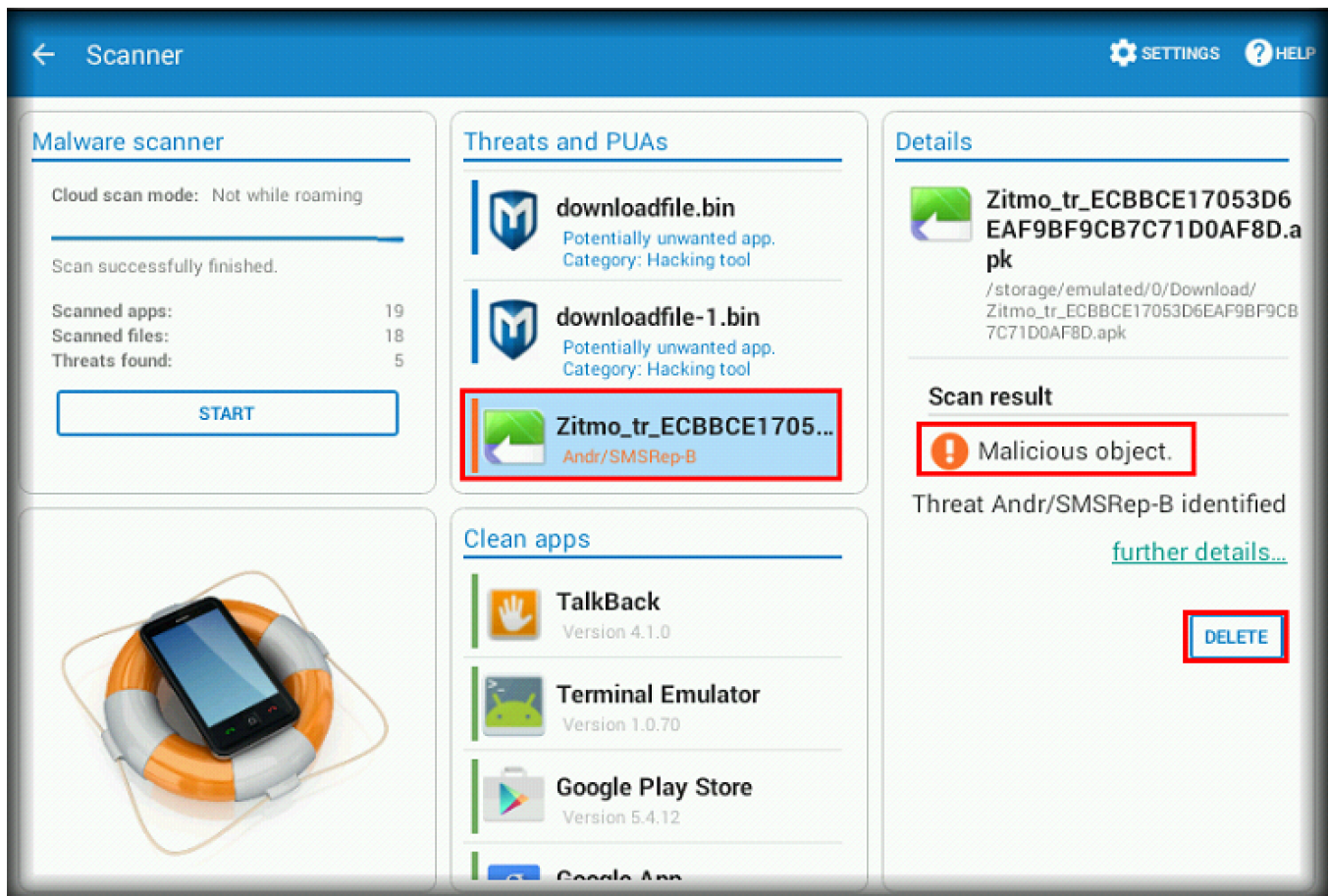


FIGURE 4.18: Deleting Malicious File

23. Now, set security settings by using Security Advisor of the Sophos Mobile Security application.
24. Click **Security Advisor** to access the settings.

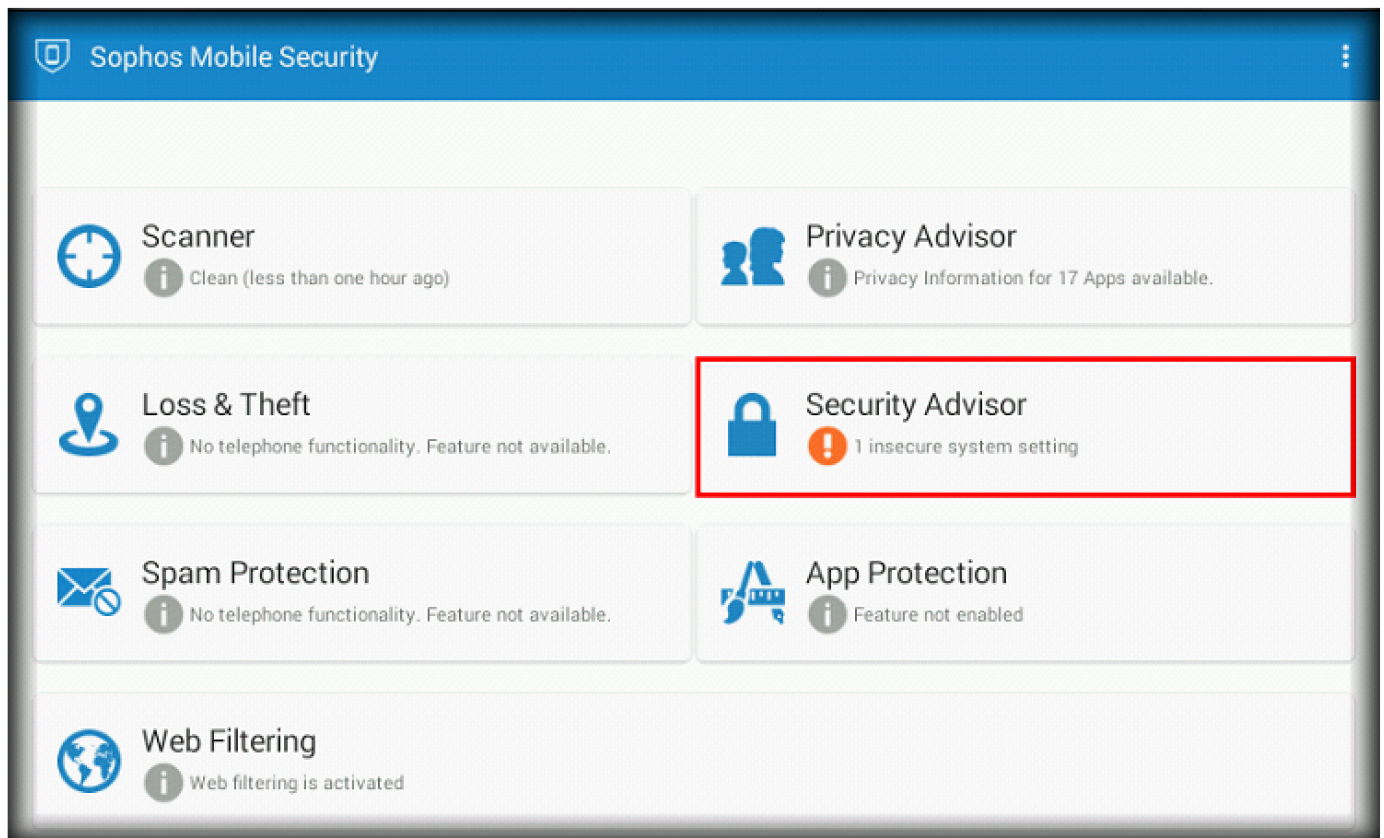


FIGURE 4.19: Sophos Security Advisor

25. In the Security Advisor window, choose **Unknown App Sources** (under Overview), and click **Change** (under Unknown App Sources).

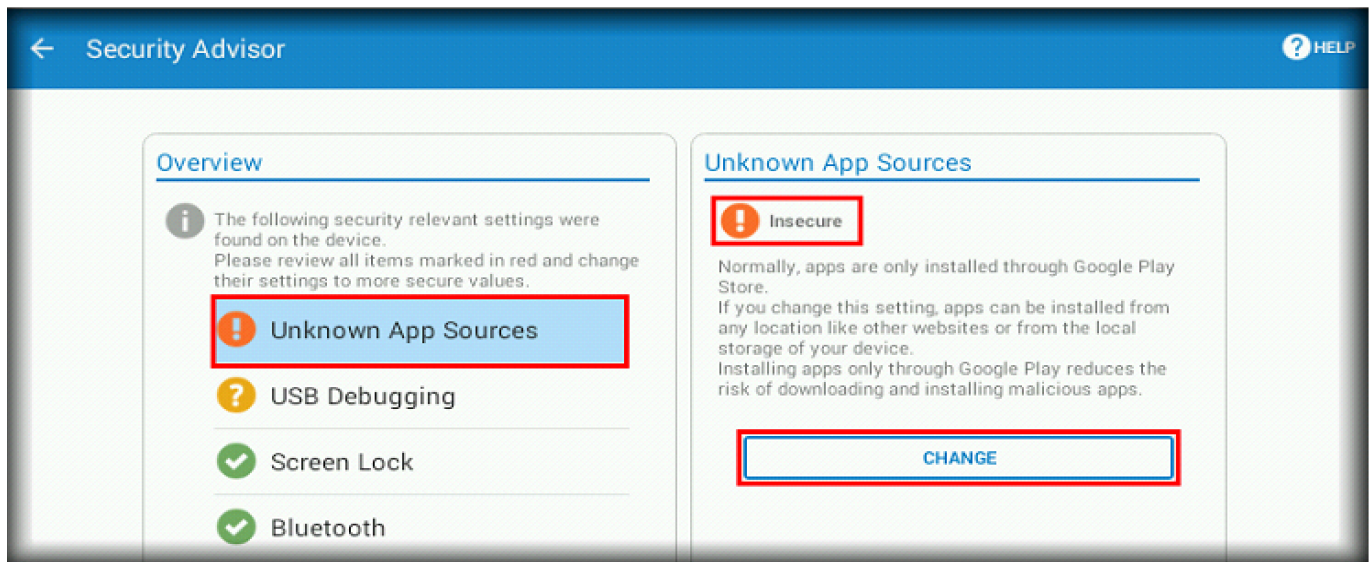


FIGURE 4.20: Changing App Source

26. The Android Security settings window appears. Navigate to **Device Administration** and choose **Unknown sources**.

27. By default, the **Unknown sources** option is checked.

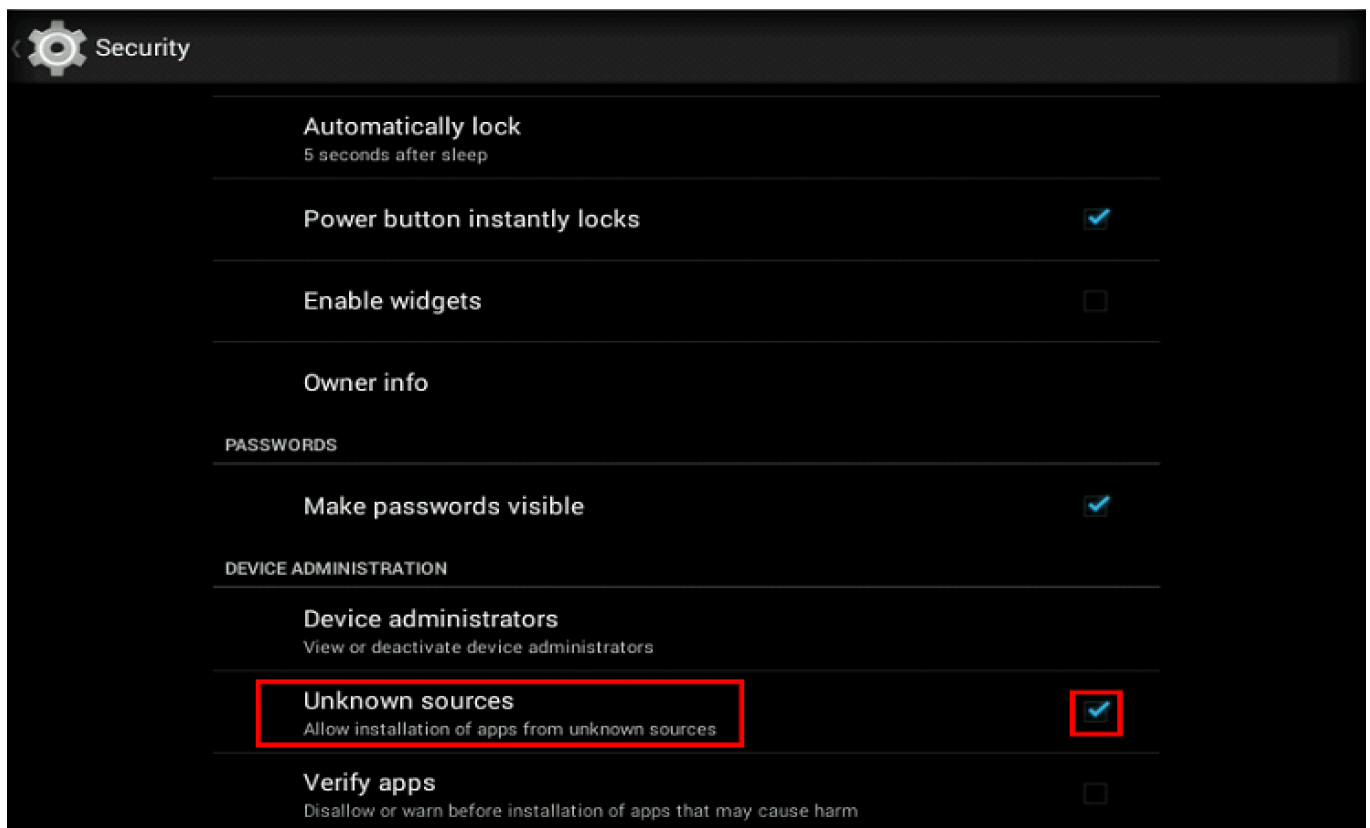


FIGURE 4.21: Android Security Settings

28. Now, **uncheck Unknown sources** (under Device Administration) to disallow the installation of apps from unknown sources.

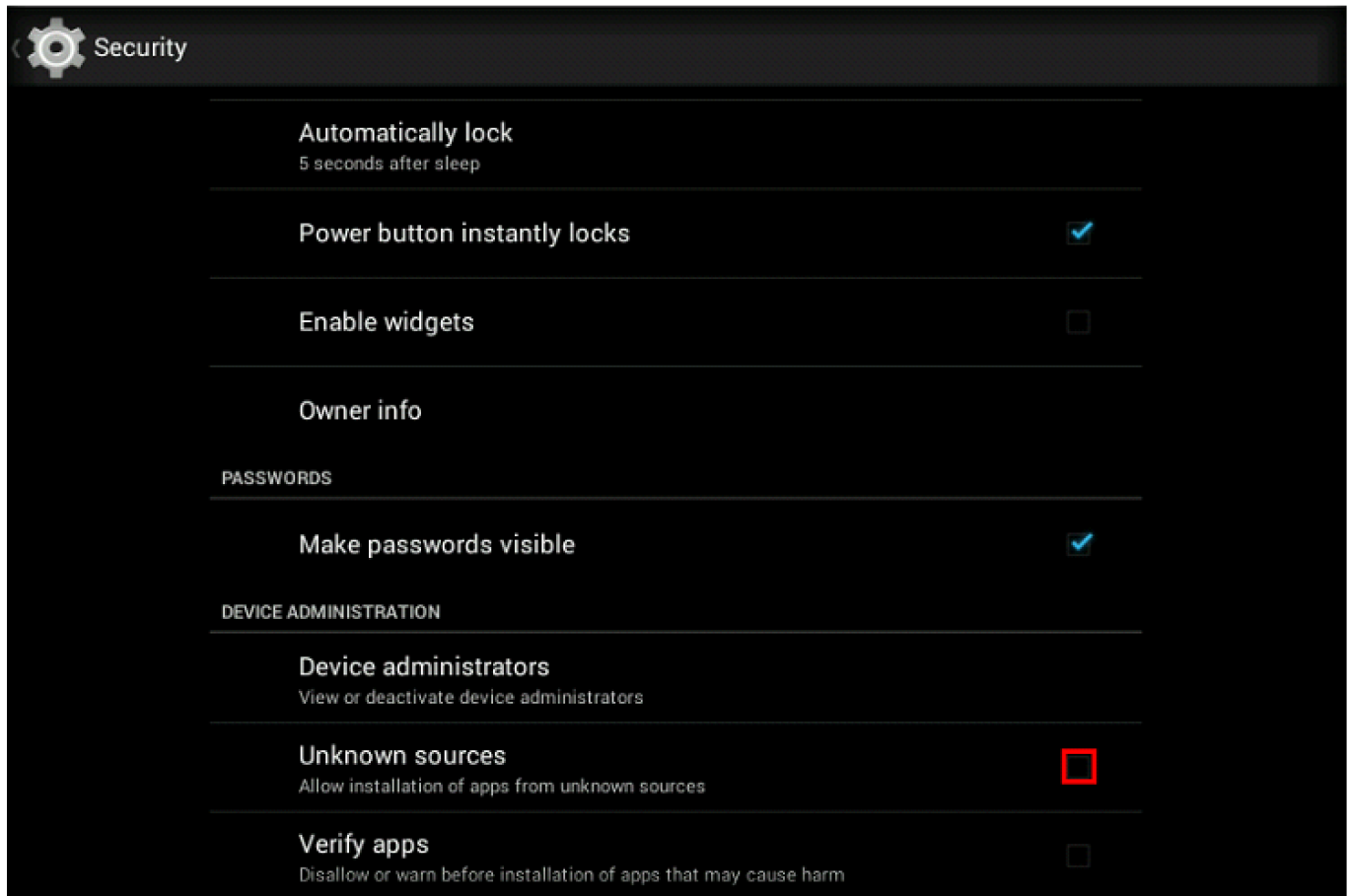


FIGURE 4.22: Android Security Unknown Services

29. Now, you can see in the Security Advisor window that Unknown App Sources is secured, as shown in the figure.

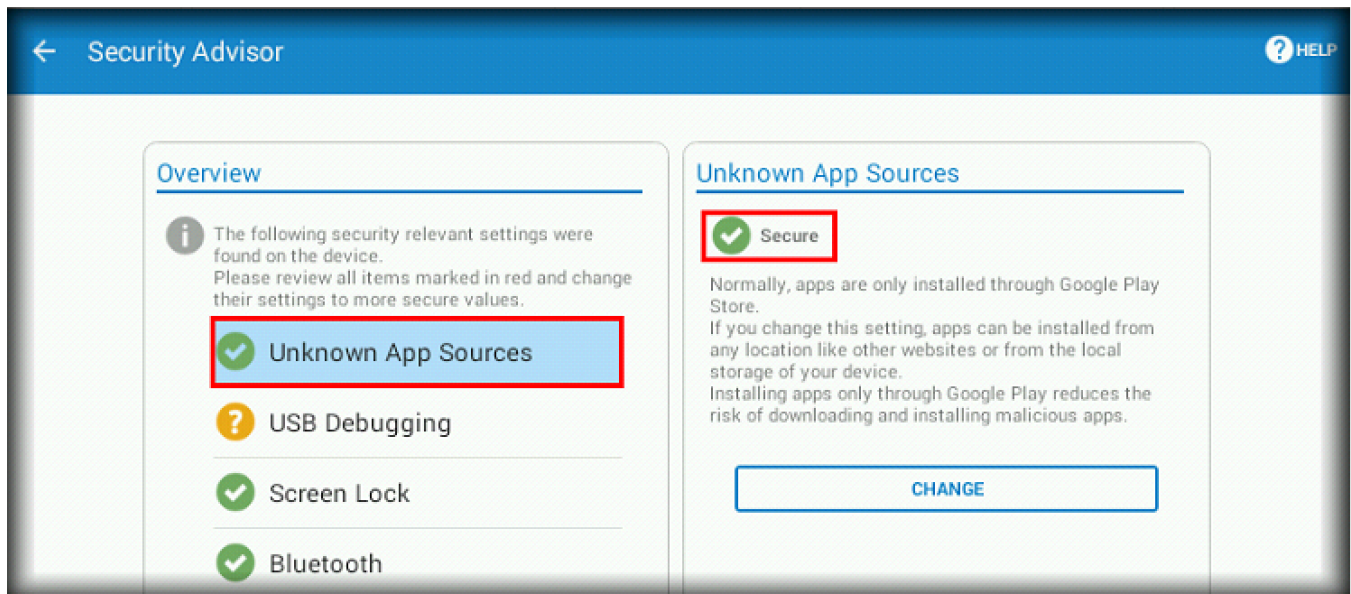


FIGURE 4.23: Unknown App Sources Secured

30. Alternatively, go through all the security options available in Sophos Mobile Security, and protect your android device from the unwanted or malicious activities.

Lab Analysis

Analyze and document your results related to this lab exercise. Provide your opinion of your target's security posture and exposure.