



Malwarebytes for Android User Guide

Version 3.3.1

20 May 2018



Notices

Malwarebytes products and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. You may copy and use this document for your internal reference purposes only.

This document is provided "as-is." The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, we would appreciate your comments; please report them to us in writing.

The Malwarebytes logo is a trademark of Malwarebytes. Windows is a registered trademark of Microsoft Corporation. All other trademarks or registered trademarks listed belong to their respective owners.

Copyright © 2018 Malwarebytes. All rights reserved.

Third Party Project Usage

Malwarebytes software is made possible thanks in part to many open source and third party projects. A requirement of many of these projects is that credit is given where credit is due. Information about each third party/open source project used in Malwarebytes software – as well as licenses for each – are available on the following page.

<https://www.malwarebytes.com/support/thirdpartynotices/>

Sample Code in Documentation

The sample code described herein is provided on an "as is" basis, without warranty of any kind, to the fullest extent permitted by law. Malwarebytes does not warrant or guarantee the individual success developers may have in implementing the sample code on their development platforms. You are solely responsible for testing and maintaining all scripts.

Malwarebytes does not warrant, guarantee or make any representations regarding the use, results of use, accuracy, timeliness or completeness of any data or information relating to the sample code. Malwarebytes disclaims all warranties, express or implied, and in particular, disclaims all warranties of merchantability, fitness for a particular purpose, and warranties related to the code, or any service or software related there to.

Table of Contents

Introduction	1
What's New	1
Background (Real-Time) Scanning	2
Getting Started	2
Correcting Initial Issues.....	4
Safe Browsing Scanner	5
Navigating the App	6
Scanner.....	7
Running a Scan.....	7
Interpreting Scan Results	7
Acting on Scan Results	9
Removing Files from External Storage (SD Card).....	10
Android version 4.4 (Kit Kat)	10
Android version 5.0 and higher (Lollipop)	12
Whitelist.....	13
Security Audit.....	13
Google Play Protect.....	13
Device Encryption	13
Installing apps from unknown sources.....	13
Development mode	13
NFC.....	13
Android Beam.....	13
Call Protection (Beta)	14
Settings.....	16
General	16
Protection Settings	16
Usage	17
Reporting Spam Callers.....	17
Your Apps	18
Privacy Audit	18
Malwarebytes Labs	19
Settings.....	19
Scanning.....	19
Protection.....	19
Real-Time Protection (RTP)	19
Anti-Ransomware Protection (ARP)	20
Scan Links Sent Via SMS.....	20
SMS Device Control	20

Table of Contents (Continued)

Other	21
Device Administrator	21
Memory Caching.....	21
Database Updates	21
Notifications	21
Help Us Anonymously	21
Share	22
About.....	22
Widgets	23

Introduction

Malwarebytes for Android ("Malwarebytes") has been designed to detect and eliminate ransomware, malware, adware, spyware and PUPs (Potentially Unwanted Programs) for mobile devices utilizing the Android operating system (version 4.4 or later). *Malwarebytes* also provides features which enable the user to control security features that affect them and their mobile device, in plain English!

FEATURE	FREE MODE	FREE + MODE (grandfathered)	PREMIUM MODE
NEW Call Protection	■	■	●
Anti-Ransomware Protection	■	■	●
Scan and Install	■	■	●
Compressed File Scanning	■	■	●
Deep Scanning	■	■	●
Scan while Charging	■	■	●
Homescreen Widgets	■	■	●
Remote Security	■	■	●
Real-Time Protection	■	●	●
Anti-Phishing Protection	■	●	●
Issue Reminders	■	●	●
Automatic Scans after Update	■	●	●
Scheduled Scans	■	●	●
On-Demand Scans	●	●	●
Improved User Experience	●	●	●
Applications Audit	●	●	●
Privacy Audit	●	●	●
Security Audit	●	●	●
Bandwidth Enhancements	●	●	●
Freeform Text Scanning (on-demand)	●	●	●

What's New

This version of *Malwarebytes* contains many improvements and bug fixes. Following is a list of changes.

Improvements

- Improved the call blocking feature
- Support for Android versions 4.3 and below is no longer available

Stability/issues fixed

- Fixed several issues that could cause the app to become unresponsive
- Fixed other miscellaneous defects

Background (Real-time) Scanning


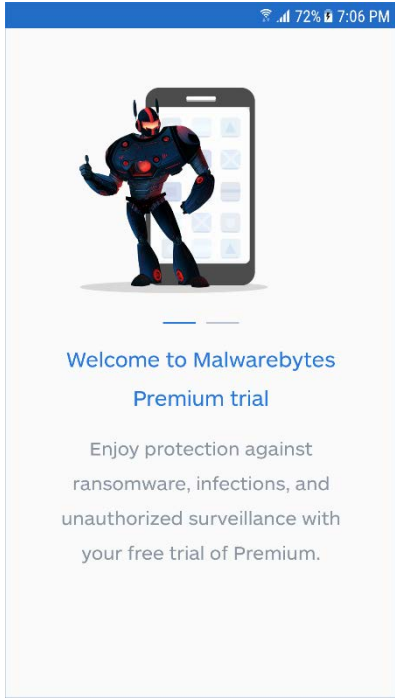
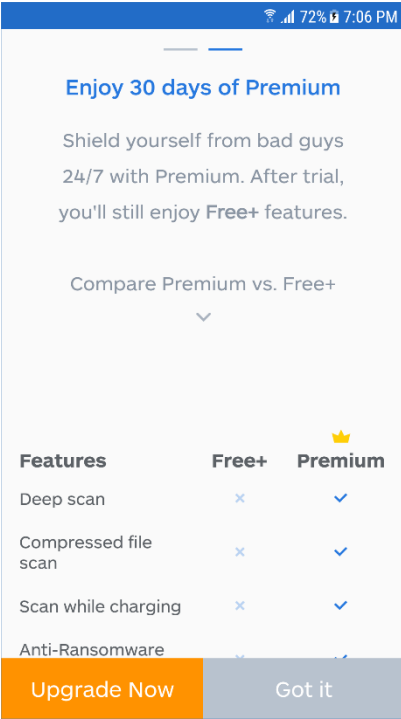
Malwarebytes will automatically perform scans in the background during normal operation. These scans occur in real-time, and are based on specific events. These events include:

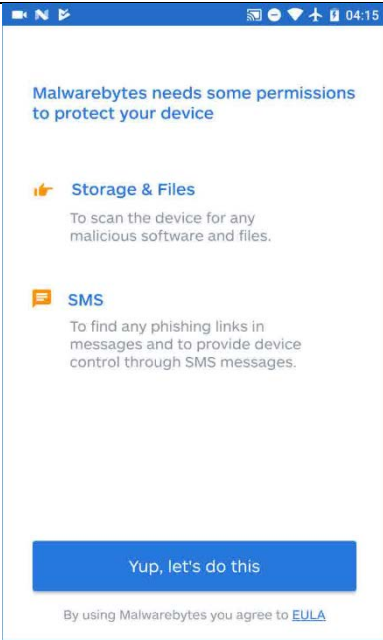
- Additions and/or modifications to files on the file system
- Downloading of files from external sources
- Installation of downloaded files
- Execution of applications
- Potentially Unwanted Programs (PUPs), based on functionality and/or behavior
- Insertion of SD memory cards
- Scan on reboot. At this time, some devices do not support this feature.

If questionable files are found during a scan, they will be brought to your attention. Deep scanning allows *Malwarebytes* to proactively scan and analyze all applications on your device, and can even find previously unknown dangerous apps which are not visible on the surface. You may whitelist, skip, or delete each item. Whitelisting a file will prevent it from appearing on subsequent scans. Skipping an item will allow it to remain, but it will be detected during the next scan.

Getting Started

The first time *Malwarebytes* is launched, it will behave a bit differently than it will from that point forward. We encourage you to read the End User License Agreement (EULA), to learn more about the value of Real-Time Protection. “Always on” protection keeps you and your device the safest. The following screenshots show what you will see the first time you launch *Malwarebytes*.

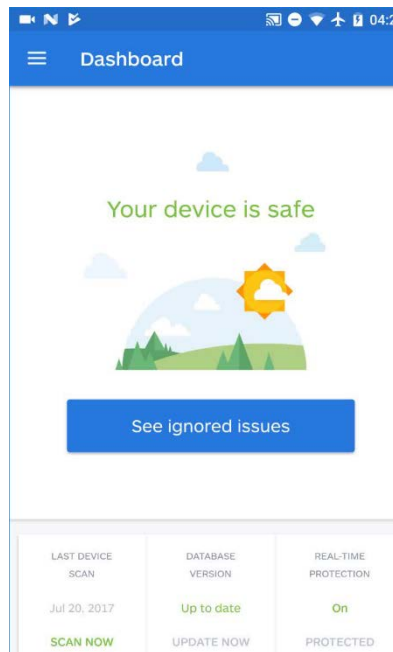
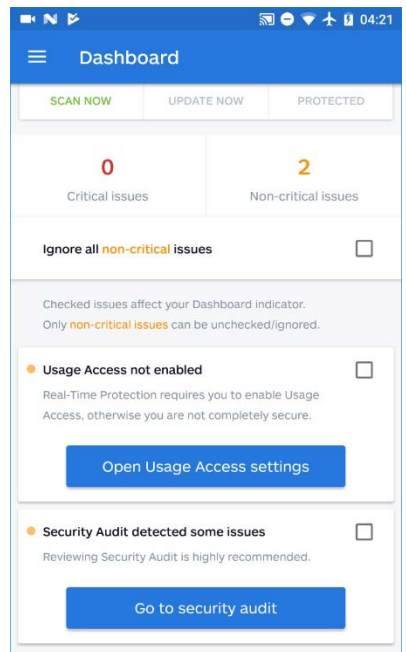
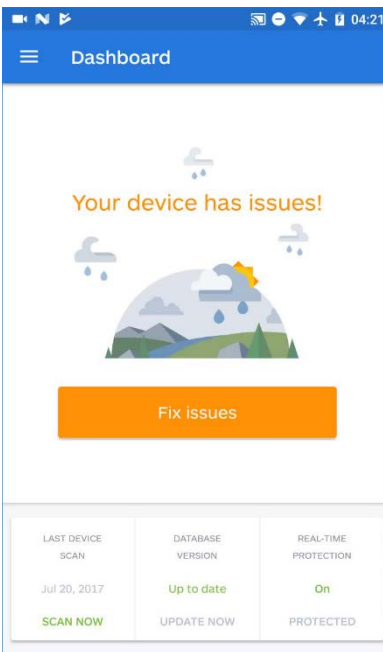
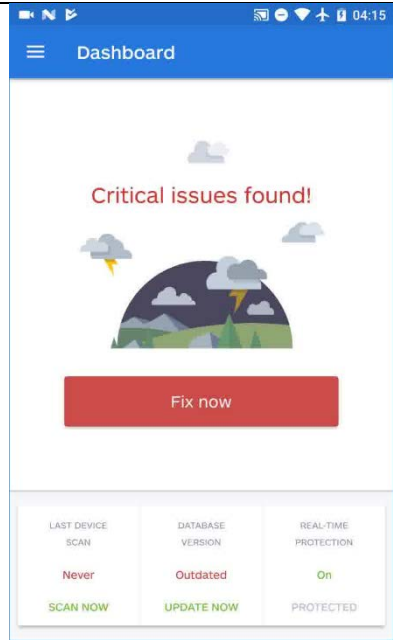
		
This is the screen you see when you launch <i>Malwarebytes</i> for the first time. Enjoy it! You'll only see it once.	You will launch into a Premium Trial that runs for 30 days. This is the first of two screens to explain the value of Premium.	Users of earlier versions start in Free+ mode. This screen shows you differences between Free+ and Premium. You can buy Premium now or continue on.



For Android 5.0 and later, *Malwarebytes* needs access to Storage and to SMS to provide Real-Time Protection for these services. We request each individually.

PLEASE NOTE that denying access to a service will limit the amount of protection that can be offered to you.

Malwarebytes will test certain important system settings, and alert you if issues are found. Critical (red) issues should be fixed immediately, while non-critical (orange) issues may be ignored if you choose. **Please note** that ignored issues may still affect the level of protection that *Malwarebytes* can offer you. Also note that your first health check after *Malwarebytes* is installed will show critical issues for the reasons shown in the screenshot.



Here is an example of an initial scan where non-critical issues were found (orange warnings instead of red, which is used for critical issues).

Scroll down to see details of the issues which were found, and how they can be corrected. Here, you can choose to fix the issues or ignore them.

Here is the end result after the issues were ignored and/or fixed. Here's more about the issues, what they mean, and how to fix them.

Correcting Initial Issues

During the health check, the “*See ignored issues*” and “*Fix issues*” message bars gave you the opportunity to look deeper at issues which *Malwarebytes* considered to be a problem. Selecting either message takes you to the **Issues** screen, shown below. Depending on the number of issues noted by the program, you may need to scroll through the list to see all of the issues. Issues are color-coded to denote their importance. Color coding appears on the bullet to the left of the message. Colors used are:

- **Orange:** Issues have been noted which may affect your security, but they are not critical.
- **Red:** Critical issues have been noted, and your security is at risk.

You will notice checkboxes to the right of each item. These checkboxes determine whether the accompanying notification will appear on the Dashboard. Red (critical) items cannot be unchecked, and are always displayed. Orange (non-critical) items may be checked or unchecked, and display of each non-critical item on the Dashboard is controlled by the state of its checkbox. Following is a list of all issues which may appear on this list, their severity, and the recommended method to correct each of them.

Last Scan Performed

Non-Critical: Last scan has been performed more than a week ago
Critical: Full scan has never been performed
Critical: Last scan has been performed more than 2 weeks ago
Resolution: Perform a full scan

Last Scan Ignore Malware (not deleted or added to whitelist)

Non-Critical: After last scan you’ve ignored some unwanted malware
Non-Critical: After last scan you’ve ignored some adware
Critical: After last scan you’ve ignored some dangerous malware
Critical: After last scan you’ve ignored some dangerous RANSOMWARE
Resolution: Perform a full scan and/or review Whitelist entries

Unscanned Apps

Non-Critical: You have new apps that haven't been scanned yet
Resolution: Perform a full scan

Old/Missing Malware Database

Non-Critical: Last malware database update has been performed more than a week ago
Critical: Malware database has not been updated yet
Critical: Last malware database update has been performed more than 2 weeks ago
Resolution: Update Malware Database

Old/Missing Malicious URL Database

Non-Critical: Last malicious URL database update has been performed more than a week ago
Critical: Malicious URL database has not been updated yet
Critical: Last malicious URL database update has been performed more than 2 weeks ago
Resolution: Update Malicious URL Database

Whitelist Cleared

Non-Critical: Whitelist that contained adware has been cleared
Non-Critical: Whitelist that contained unwanted malware has been cleared
Critical: Whitelist that contained dangerous malware has been cleared
Critical: Whitelist that contained dangerous ransomware has been cleared
Resolution: Perform a full scan

Scans Disabled

Non-Critical: Scan after update is disabled
Resolution: Enable this setting to assure you are protected with the newest threat information

Real-Time Protection Disabled

Non-Critical: Real-Time Protection is disabled

Resolution: Enable Real-Time Protection

Security Audit Issues

Non-Critical: Security Audit detected some issues

Resolution: Reviewing Security Audit is highly recommended

Permissions

Non-Critical: Device Administrator is not enabled (affects ransomware protection)

Non-Critical: Access SMS denied (affects SMS phishing protection)

Non-Critical: Usage Access not enabled (affects display of Installed Apps)

Non-Critical: Safe Browsing Scanner Disabled

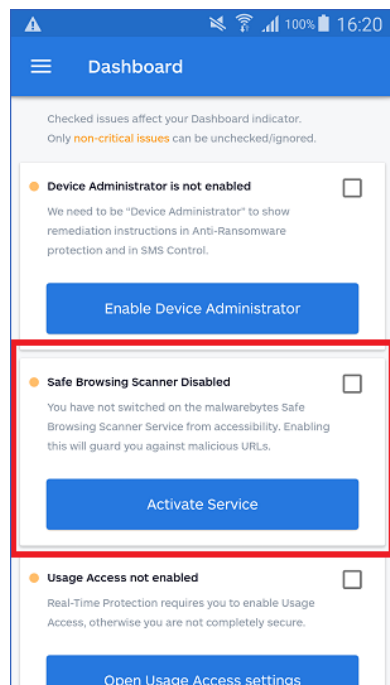
Critical: Access Storage denied (affects real-time protection and scanning)

Critical: "Draw over other apps" disabled (affects ransomware protection)

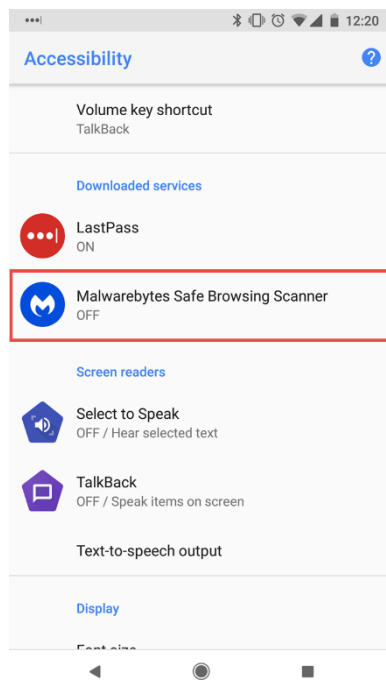
Resolution: Enable settings to enable protection for each reason shown here.

Safe Browsing Scanner

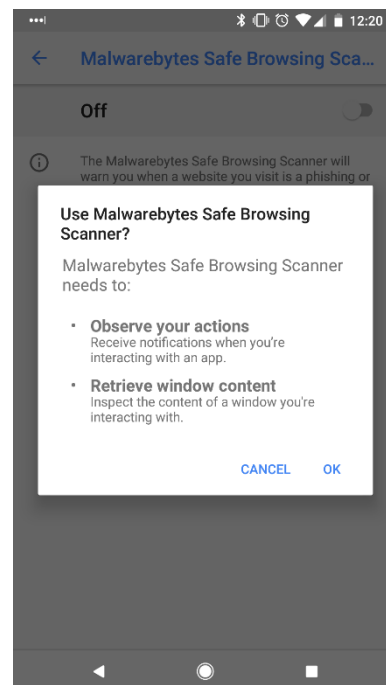
Computer-based Internet users have long been faced with websites serving malware and phishing links, mostly in attempts to gain access to confidential information. The issue is magnified on smartphones and tablets due to the prevalence of younger users. To combat this threat, *Malwarebytes* has introduced the Safe Browsing Scanner for users of *Malwarebytes Premium*. In combination with real-time protection, the Safe Browsing Scanner inspects web page content and alerts you to the presence of dangerous content.



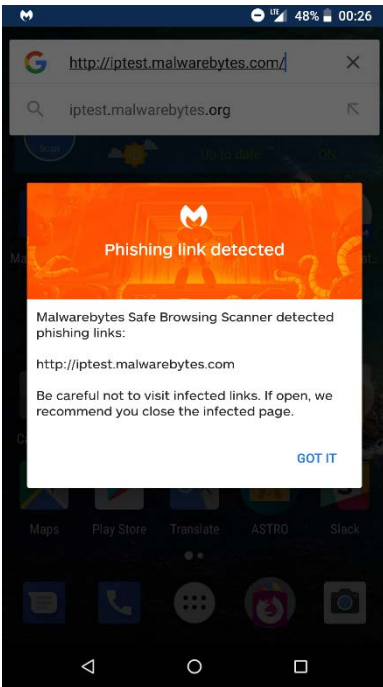
Malwarebytes Premium users will see this issue listed in their Dashboard. Click **Activate Service** to use the Safe Browsing Scanner.



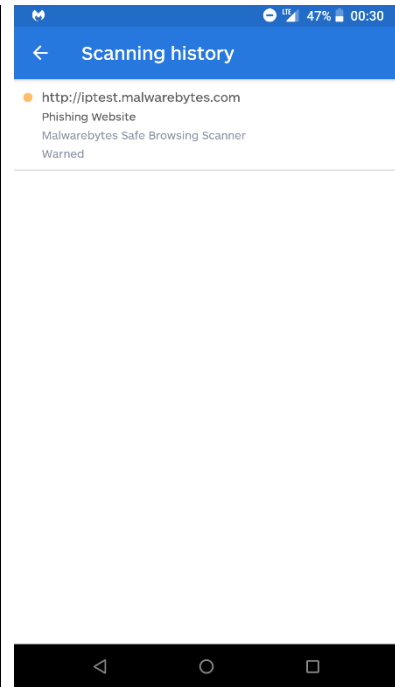
This Android system screen shows the status of the Safe Browsing Scanner, and will update when it is activated.



This screen shows how you authorize Android to allow the Safe Browsing Scanner to protect you.



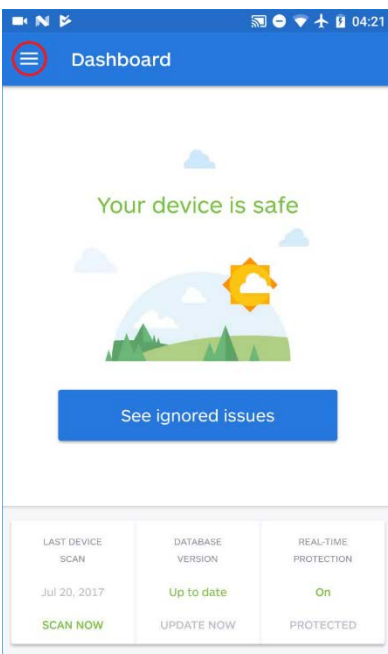
When a malicious link is detected, this warning will be displayed, and persist until you close it.



In addition, your Scanning history will show a record of the malicious link which was blocked.

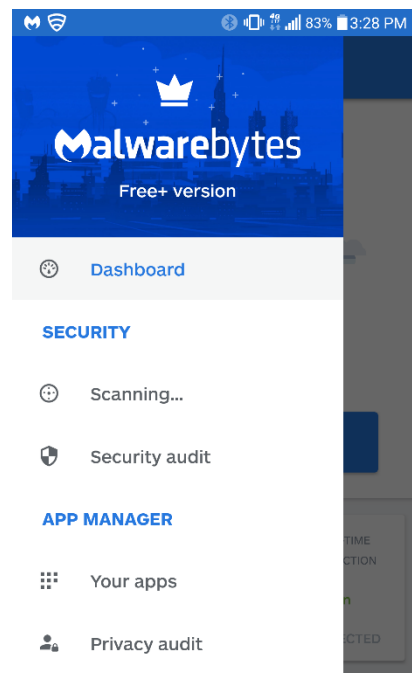
Navigating the App

Once *Malwarebytes* has been installed on your device, it can be launched from the notification bar at the top of your screen, as well as from your Apps screen. You may configure the notification bar icon to be hidden as well...more on that later. The following screenshot shows the presentation of *Malwarebytes*.



The **Dashboard** (left) is the entry screen for *Malwarebytes*, and serves as a starting point for everything else you need to do within the program. It shows status information for your device. It runs a health check every time you land on the screen to keep you informed. Notice the red circle in the upper left corner. Swipe it to see the program menu (shown on the right).

The program menu gives you access to all functionality of *Malwarebytes*. The **Free+** version of *Malwarebytes* is shown here. **Free+** and Premium share the same menu, while the Free version has a more limited menu.



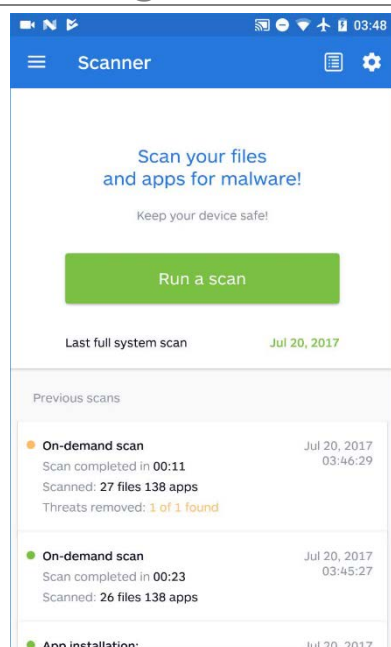
Scanner

These settings allow you to define how and when *Malwarebytes for Android* will scan your system for malware, what to do if malware is found, and what – if anything – it should ignore.

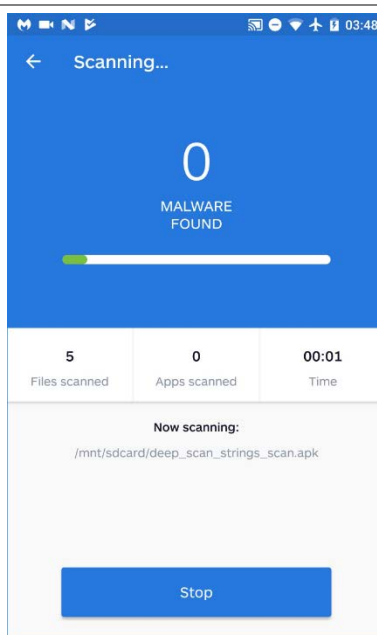


Before going any further, two settings at the top of the Scanner page should be mentioned. **Whitelist** is used to exclude some files from being scanned as part of a normal scan. **Scan Settings** allow you to define if scheduled scans are to be performed, when they are to be performed, and if scans should be run based on certain device events. **Whitelist** is covered on page 11 and **Scan Settings** are covered on page 13.

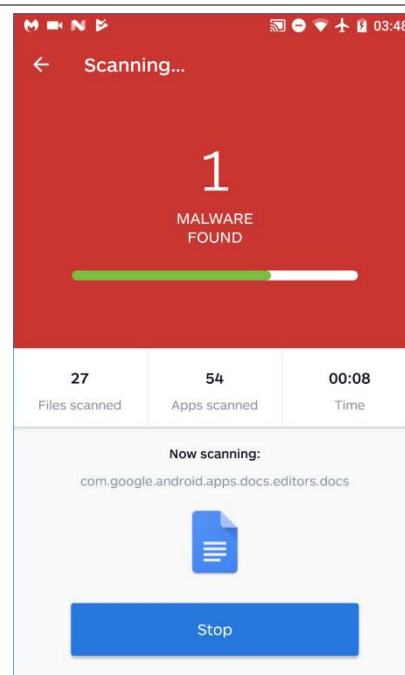
Running a Scan



When **Scanner** is selected from the Program Menu, you will see this screen. Previous scan results will be shown. You can swipe across a result to remove it from your screen. Press **Run a scan** to begin.



This screenshot shows a running scan. No malware has been detected...yet.



When malware is detected, you will see the screen change as shown. The scan will continue on and provide a count of how many threats were detected.

Interpreting Scan Results

When looking at Scan History, you will notice a number of similarities between scan results. We thought it might be helpful to document the results you will be seeing. Please note that the same topic may appear with different color bullets in front of the text. As mentioned earlier, green is good, orange is a non-critical issue, and red is critical. Here are the scan results:

In this section, references will be made to whitelisting, ignoring and deleting files. Those will be covered in detail in the following section.

On-demand scan

- **Green:** An on-demand (non-scheduled) scan ran to completion with no issues detected. Please note a scan which did not detect any issues **and** was canceled by the user before it was complete will not be reported. There is also no assurance that the device is actually issue-free if the scan was not allowed to complete.
- **Orange:** PUPs were detected during an on-demand (non-scheduled) scan. If the scan was canceled before it was complete, there may be more PUPs present than what is reported in results. You must whitelist, ignore or delete files causing this alert.
- **Red:** Malware was detected during an on-demand (non-scheduled) scan. If the scan was canceled before it was complete, there may be more malware present than what is reported in results. You must whitelist, ignore or delete files causing this alert.

Scheduled scan

- **Green:** A scheduled scan ran to completion with no issues detected.
- **Orange:** PUPs were detected during a scheduled scan. You must whitelist, ignore or delete files causing this alert.
- **Red:** Malware was detected during a scheduled scan. You must whitelist, ignore or delete files causing this alert.

Scan after update

- **Orange:** A scan was executed after the signature database was updated. PUPs were detected. You must whitelist, ignore or delete files causing this alert.
- **Red:** A scan was executed after the signature database was updated. Malware was detected. Pups may also be present. You must whitelist, ignore or delete files causing this alert.

SMS scan

- **Orange:** An SMS scan detected a phishing link.

SD-card scanner

- **Orange:** A scan of a SD memory card being inserted into the device resulted in PUPs being detected.
- **Red:** A scan of a SD memory card being inserted into the device resulted in malware being detected. PUPs may also be present.

Reboot scan

- **Orange:** A scan was executed after a device reboot, and PUPs were detected.
- **Red:** A scan was executed after a device reboot, and malware was detected. PUPs may also be present.

File monitor

- **Orange:** Real-Time Protection detected PUPs during a file transfer. You must whitelist, ignore or delete files causing this alert.
- **Red:** Real-Time Protection detected malware during a file transfer. PUPs may also be present. You must whitelist, ignore or delete files causing this alert.

App installation: <filename>

- **Orange:** Real-Time Protection was triggered by installation of a file identified as a PUP. You must whitelist, ignore or delete the file.
- **Red:** Real-Time Protection was triggered by installation of a file identified as malware. You must whitelist, ignore or delete the file.

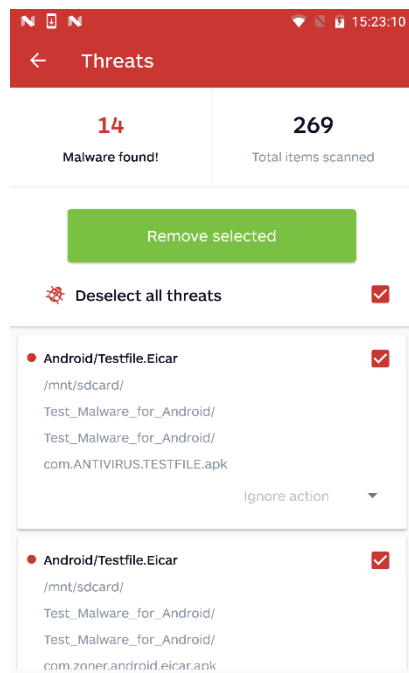
App execution: <filename>

- **Orange:** Real-Time Protection was triggered by execution of a file identified as a PUP. You must whitelist, ignore or delete the file.
- **Red:** Real-Time Protection was triggered by execution of a file identified as malware. You must whitelist, ignore or delete the file.

Acting on Scan Results

If you run a scan and the scan does not detect any malware, you're safe for the time being. If malware is detected, it needs to be dealt with. You have three choices:

- **Delete** – The threat will be deleted from your device
- **Ignore Always** – The file which has been detected as a threat will be added to a Whitelist, and excluded from future scans. Legitimate files are sometimes detected as malware. There may also be files which are classified as PUPs that you want to use. These are examples of files to be excluded from scanning.
- **Ignore Once** – A file has been detected as a threat, but you're not sure whether it should be added to a Whitelist or deleted. You choose to ignore it this time only. It will be detected as malware on your next scan, and this scan to be shown as red status, because malware remains after the scan results have been processed.



This is a typical view of **Scan results** after a scan has been completed and malware has been detected. Please note that all items have been checked. (While we can only see two items here, the *Deselect all threats* choice in the upper right means that all malware detected has been selected.

Pressing *Deselect all threats* will remove the checkmarks from all files, and change the option from *Deselect all threats* to *Select all threats*.

As stated above, you can choose to delete threats, ignore them once, or ignore them always. For each disposition, select the file(s) from the list and choose what you want to do with them. You will be asked to confirm your choice, and if confirmed, your choice will be acted on. The file(s) will be removed from the list, leaving only files which still need to be acted on.

Choose the files which will be handled in the next method. If your first action was to delete threats, you would now choose which should be ignored always. If any files are left over, choose to delete them or to ignore them this time only.

You should not leave any threats outstanding without choosing how they should be handled.

There may be times that files cannot be deleted after a scan. This may occur for the following reasons:

- Files may reside in system folders
- They are locked or in use by other apps
- *Malwarebytes for Android* was not given storage permissions (or permissions were revoked)
- Files are bloatware installed on the device by the vendor.

If this situation occurs, you will see an error indication when you try to delete a file of this type. To find the location/path of the file, tap on the scan history (available in *Menu ► Scanner*). This will display all files and apps detected for that particular scan.

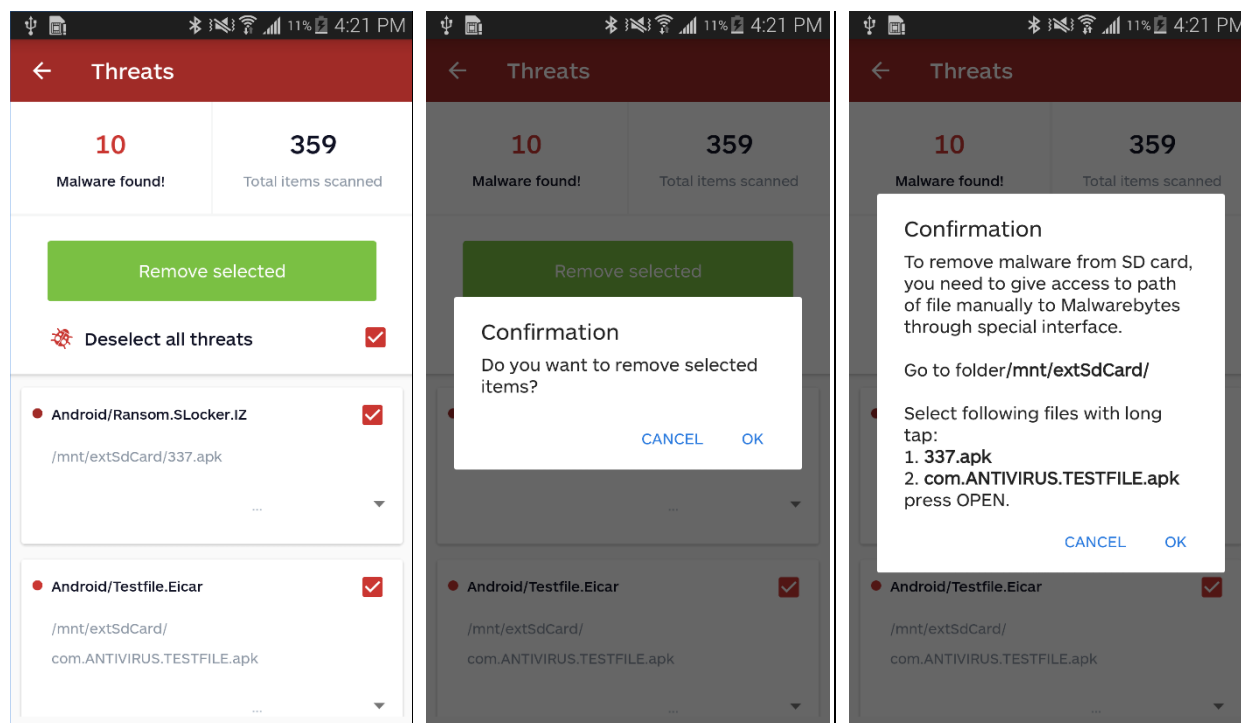
Removing Files from External Storage (SD Card)

Beginning with Android version 4.4 (Kit Kat), Google restricted methods that applications could use to access files on external storage (SD cards). With the introduction of Android 5.0 (Lollipop), access methods changed again. This time, access became easier. Below, you will find detailed instructions on how to remove malware from SD cards on the various Android versions.

Android version 4.4 (Kit Kat)

To remove a malicious file from external SD card storage on a Kit Kat device, direct access to the file is required by the app. The user must manually provide access to *Malwarebytes*, using a special file selection interface.

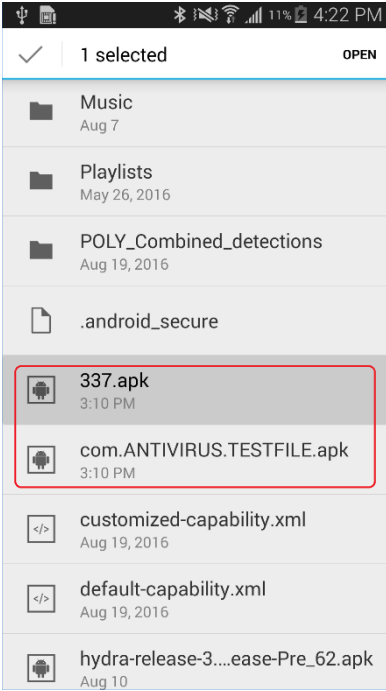
When the user requests that malware found by a scan be deleted (regardless of whether it is in internal or external storage), *Malwarebytes* will display a confirmation dialog. This dialog contains information about the folders containing malware, and will be displayed until all malware has been deleted or until the user cancels delete operations in that folder. The next folder containing detected malware will then be displayed. This will continue until all affected folders have been cleaned or skipped by the user.



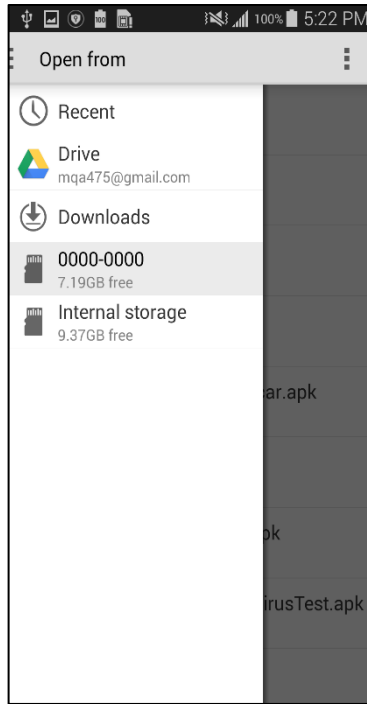
After the scan completes, select the file(s) to be removed and press **Remove Selected**.

Confirm delete operation for selected malicious files.

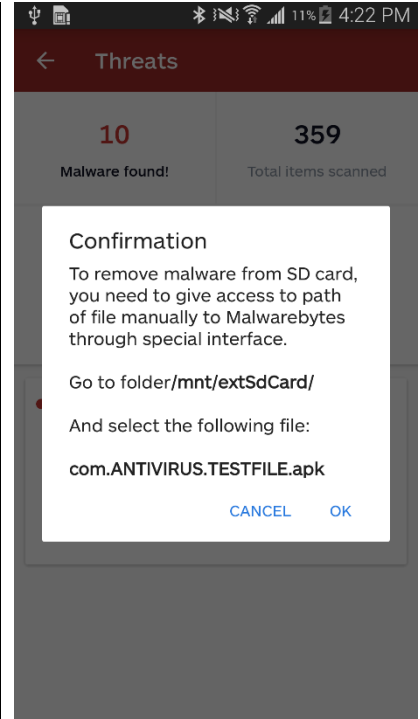
This dialog will display If malware is present on the SD card. The folder containing malware and the malicious files will be listed.



Find files displayed in the previous dialog. **Please Note:** Only files identified in dialogs as malicious can be deleted.



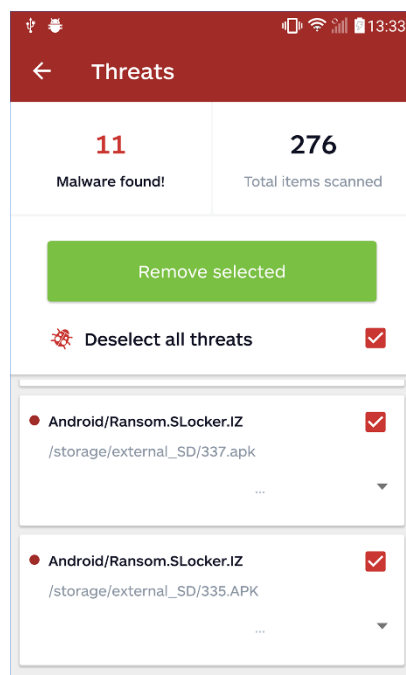
The user can use the navigation drawer (sidebar) to choose external storage if it is not selected by default.



If only the first file was selected for removal, you will be requested to handle the second file identified as malware.

Android version 5.0 and higher (Lollipop)

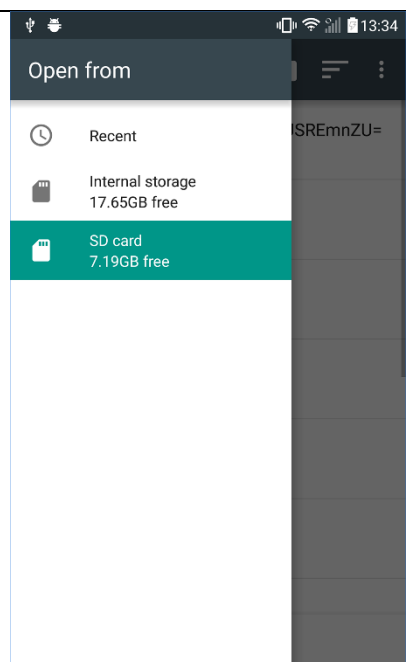
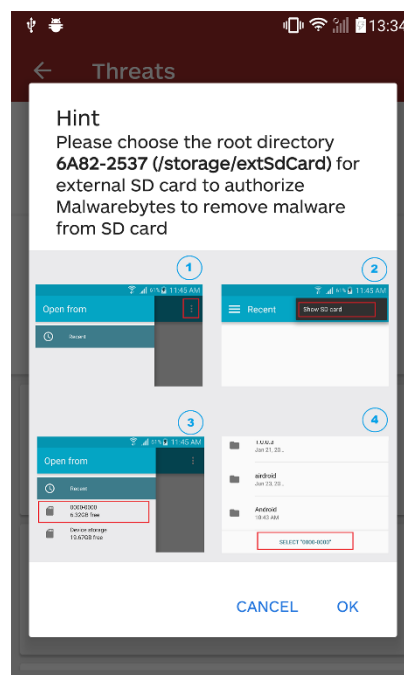
Removing files from SD card on Lollipop devices is easier. To enable *Malwarebytes* to remove malware from SD card, the user should provide the app access to the whole external storage manually. This access only needs to be given once (per installation or clearing data). It should be given manually through the special interface provided by Android. Within that interface, the user must select the root folder of the SD card. That provides *Malwarebytes* with the permission required to remove malicious files from SD card. And in further no special actions are needed from user, like it does on prior KitKat devices.



After scan completes, choose to **Remove selected** malware files. You can select one or all files for removal.

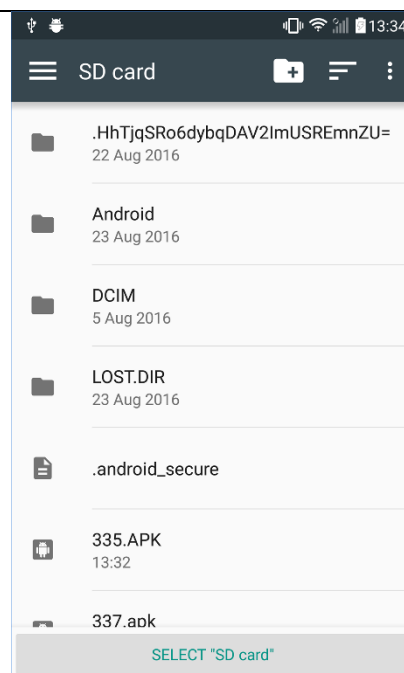
After confirming that you wish to delete files, a screen showing instructions will guide you to grant permission to Malwarebytes to access your SD card. Press OK after reading the instructions.

The “burger” button in the upper left corner of the Recent screen can be pressed to open the sidebar. You can also swipe from the left edge towards the center of the screen to open the sidebar.



Select the SD card, as shown at left.

And finally, select the SD card's root folder as shown on the right screenshot.



PLEASE NOTE: The name given to the SD card can vary from device to device. By pressing SELECT <root folder>, –the user gives app access to remove malicious files from entire SD card. Files will be deleted immediately after access is granted. Permission to access the SD card persists until the app is uninstalled, or its data will be cleared.

Whitelist

If a file/app appears on the Whitelist, it is considered safe only because you said it is safe. Files/apps may only be added to the Whitelist as part of processing malware detected during a scan.

If you have added a file/app to the Whitelist and later decided that you do not wish it to be excluded from scanning, select the checkbox next to the file/app and press **Remove from whitelist**. It will be removed immediately.

You may remove all files/apps from the Whitelist by pressing **Select all** at the top right, followed by **Remove from whitelist**.

Once a file/app has been added to the Whitelist, it will remain there until you remove it, or if *Malwarebytes* has determined that the file has changed. This may be because its signature has changed (possibly indicating active malware in the file/app), or because the file/app has been updated.

Security Audit

This feature provides capability to enable different Android options which enhance your personal privacy and security. Options shown are dependent on features which the mobile device offers. All features will be shown as Secure Settings or Insecure Settings, based on whether their current state implies a security risk for the device and the user.

Google Play Protect

Android 8 (Oreo) introduced this optional feature to test apps to assure they are not malicious. While you can use *Malwarebytes* without enabling this feature, it is in your best interest to protect yourself in every way possible.

Device Encryption

This feature allows encryption to be enabled on your device, thus safeguarding your data.

Installing apps from unknown sources

This feature allows you to choose whether to install apps from any source, or only from approved sources. The specific screen name shown will vary depending on the mobile device used.

Development mode

This feature maps to the Android Developer Options screen, which allows a device to be used as a development platform. This mode disables many security features, allowing developers to control these features programmatically. Presence of this feature is dependent on hardware and software which supports this feature.

NFC

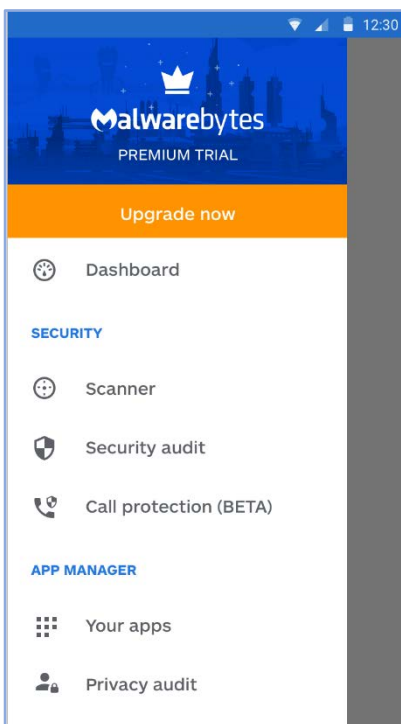
This feature maps to the Android Wireless/Networks screen, which allows communication with another device using Near Field Communication (NFC). Presence of this feature is dependent on hardware and software which supports this feature.

Android Beam

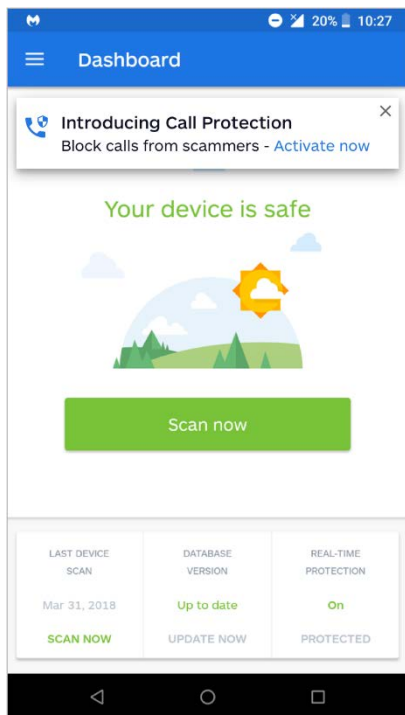
This feature maps to the Android Wireless/Networks screen, which allows a device to be able to transfer information to/from another Android device if Near Field Communication (NFC) is enabled. Presence of this feature is dependent on hardware and software which supports this feature.

Call Protection (Beta)

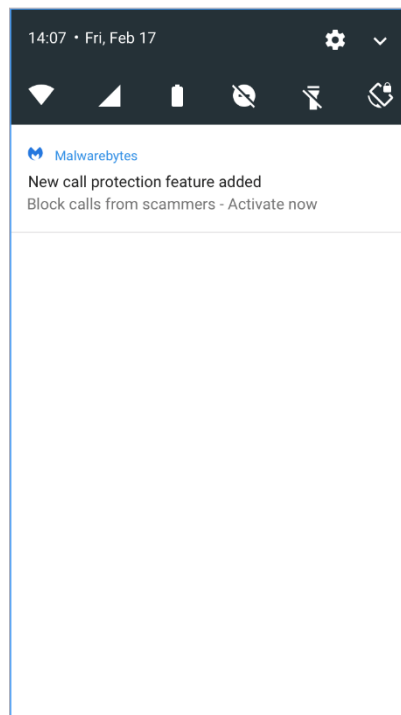
This feature is available to Premium and Trial users only. When enabled, Call Protection helps prevent spam or spoof calls to your device. Please note that the Beta test of this feature supports US numbers only. A future update will include support for International numbers. There are several ways to access this feature, as shown in the images below.



Select Call protection (BETA) from the program menu.

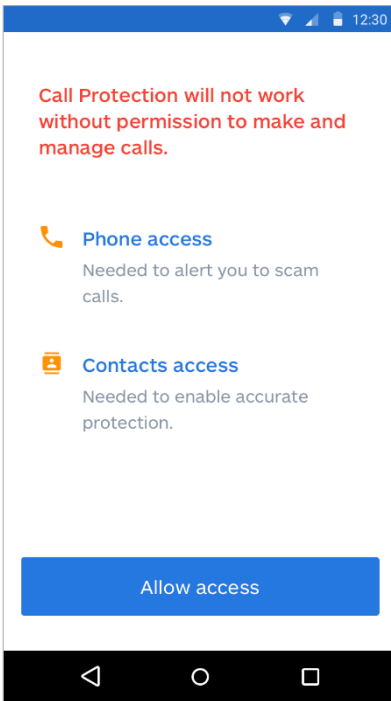


In-app notification of Call Protection.

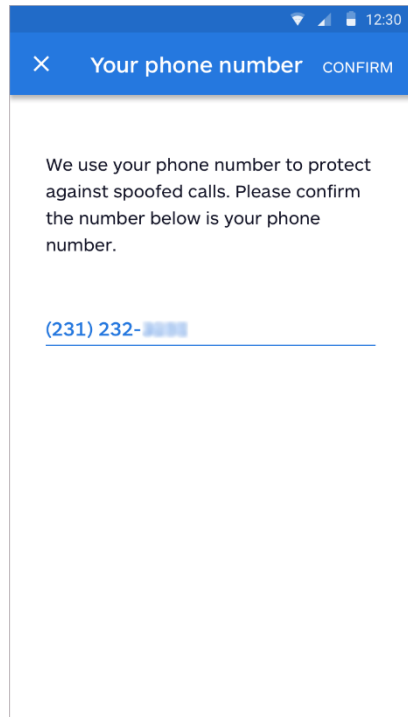


Push notification of Call Protection.

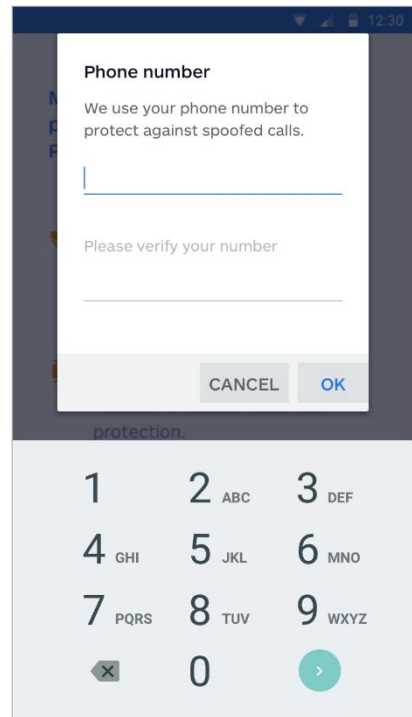
When you select any of these options, you will see a screen describing the benefit of activating Call Protection. If you are a Free or Free+ user, you will need to upgrade to Premium to use this feature. Premium users will be able to activate the feature from this screen. Once you have activated Call Protection, you will need to grant *Malwarebytes* access to your Phone and Contacts. We require these permissions to be able to effectively protect you against spam calls while still allowing your contacts to be able to reach you. Finally, you will need to confirm your phone number. Many spam callers will attempt to call you using a phone number that is similar to yours, making them seem more trust-worthy. By confirming your phone number, we can help prevent these spoof calls. *Malwarebytes* will attempt to automatically fill your phone number. If the number shown is incorrect, or if the program is unable to locate your phone number, tap on the screen to edit the number. This initial setup is shown in images below.



Malwarebytes will request access to your Phone and Contacts. If you do not provide access, the program will not be able to provide protection.

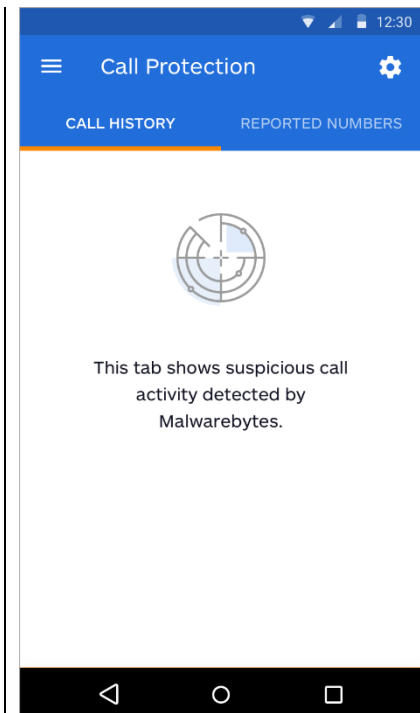


You will need to confirm your phone number to protect from spoof calls that impersonate a local number.

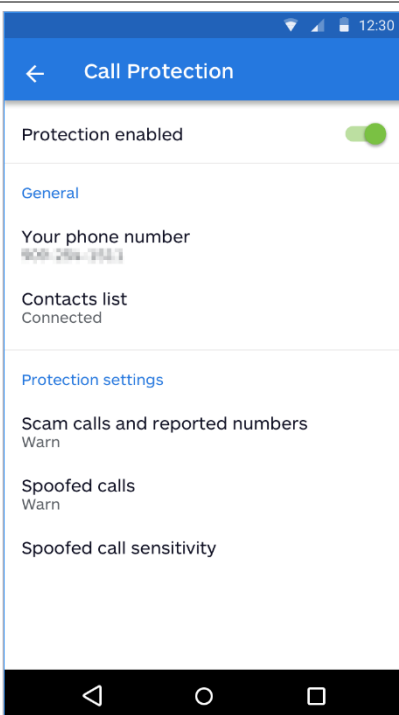


You may need to confirm or edit your phone number.

Call Protection is now active on your phone. Your phone will show the Call Protection Dashboard. Before we discuss the feature fully, we will look at the Call Protection Settings so you can understand what options you have to customize your protection.



Settings



This screen shows the Call Protection Settings. You can choose to use Call Protection as is, with the default settings, or you may adjust the protection further. Tap the gear icon in the upper-right corner of the Call Protection Dashboard to be taken to the settings menu for Call Protection. Call Protection settings are divided into two groups – General settings and Protection settings.

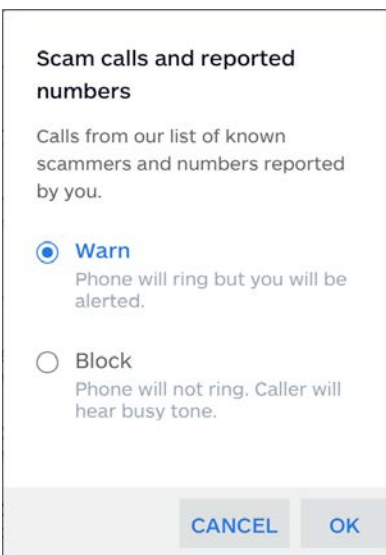
General

The General settings allow you to set your phone number and connect your contacts list. You may already have done this while setting up Call Protection. If you have not provided access to your Contacts List, you do this any time by tapping the Contacts List option from this menu. Similarly, if you want to add or change your phone number, you can do so by tapping the option in the menu.

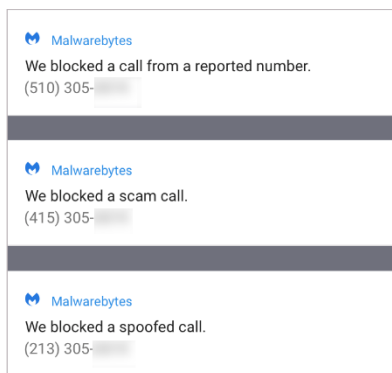
Protection Settings

The Protection Settings allow you to fine tune the level of protection from spam callers *Malwarebytes* provides. Calls are broken into two categories – Scam calls and reported numbers and spoofed calls. Scam calls and reported numbers are known malicious callers or phone numbers collected and verified by *Malwarebytes*. Spoofed calls are potentially spam calls that come from phone numbers that begin with the same numbers as yours. This is done to make the call look like a local caller. Typically, malicious callers will use a large pool of similar numbers, making blocking individual numbers ineffective.

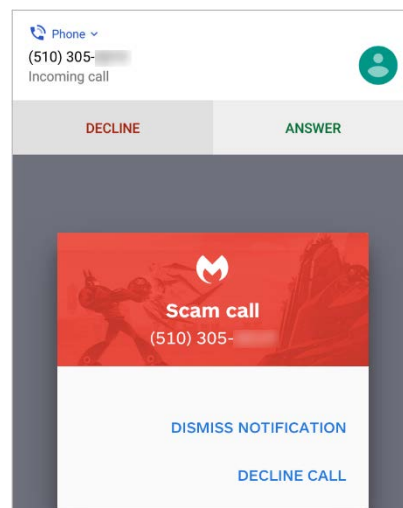
For both category of calls, you can choose whether *Malwarebytes* will **Warn** you about the call, or **Block** the call. You can set each category separately. If a call is blocked, the phone will not ring, and the caller will get a busy tone. Your phone will display a push notification to let you know a call was blocked. If you set *Malwarebytes* to **Warn**, your phone will ring and you will see an alert that *Malwarebytes* has detected a scam call. We leave the choice to answer the call up to you. These notifications are shown below.



You can toggle between **Warn** and **Block** for either type of spam caller.



Blocked calls do not ring on your phone. You will see a push notification when a call is blocked.



If set to **Warn**, you will have the choice to answer or decline the call. *Malwarebytes* will warn you of the potential threat.

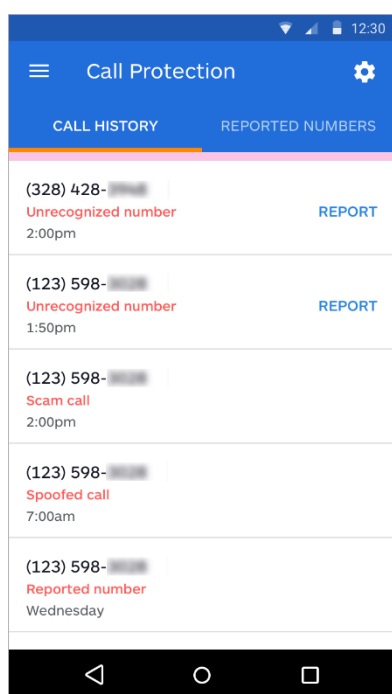
Usage

Now that you have activated the feature and have configured the settings, you can begin using Call Protection. The feature is mostly automatic – you will rarely need to take any further action after setup. The Call Protection Dashboard has two displays – [Call History](#) and [Reported Numbers](#). Call History will display a history of any calls that triggered a block or warning. You may also see calls listed as **Unrecognized Number**. These calls are from numbers that are not in your Contacts list, nor recognized by *Malwarebytes* as spam or spoof callers. If you suspect this number is a spam caller, you can help us by reporting the number. Reported Numbers shows a list of all the phone numbers you have reported to *Malwarebytes* as spam.

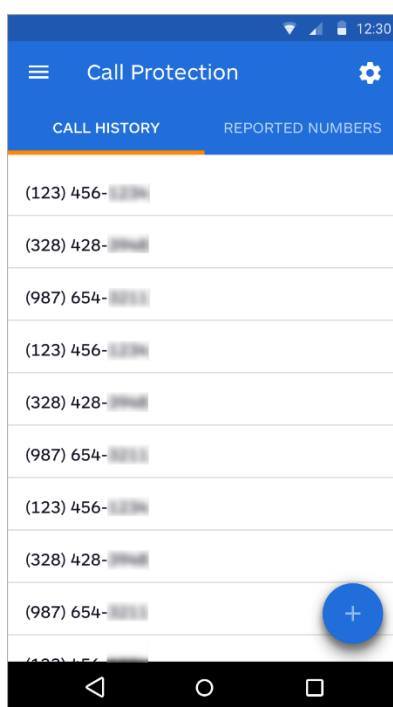
Reporting Spam Callers

There are two methods to report calls you think are Spam. These two methods are:

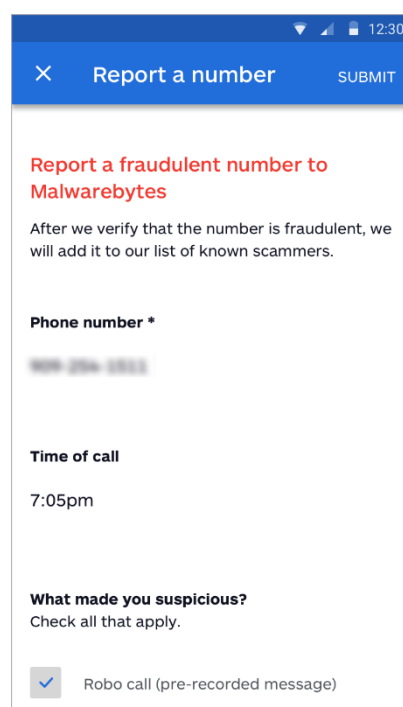
- **Reporting a call from Call History:** You can report Unrecognized Numbers from the Call History menu inside the Call Protection Dashboard. Tap the [Report Number](#) link next to an Unrecognized Number to open the form. The number you are reporting will be pre-populated into the form.
- **Reporting a number manually:** If you wish to report a number that has not called you, you can manually enter the phone number from the Reported Numbers menu. Tap the + icon in the bottom right corner of the Reported Numbers menu. You will need to enter all information about the phone number you are reporting.



The Call Protection Dashboard will show you all spam or spoof calls. You can tap **Report** next to a number to submit it to *Malwarebytes* for analysis.

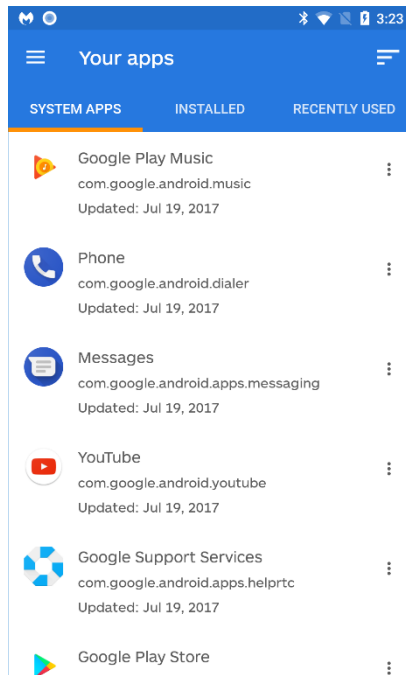


The Reported Numbers menu shows all the numbers you have reported to *Malwarebytes* as spam. You can report a new number by tapping the +.



When you report a number, we ask that you provide as much detail as you can. This helps us confirm if a number is fraudulent or not.

Your Apps



Your Apps is divided into three groups: **System apps**, **Installed apps**, and **Recently Used** apps. **System apps** are installed by Google as part of the Android operating system. **Installed apps** are installed by you. **Recently Used** are apps that have been used recently, and may be either System apps or Installed apps. We can only provide usage information if you have granted *Malwarebytes* usage access.

Press the three bars at the upper right of the screen to change the way apps are sorted. Press the three dots next to any app to uninstall, view App Info, or open it in the Play Store. You may also get App Info by pressing the name of the app itself.

This screen shows app memory usage characteristics, and provides options affecting operation of the app. These options include:

- Force Stop
- App info
- Uninstall
- Clear Data
- Clear Cache

Please note that **App info** is an Android system utility. It provides deeper access into how apps function, and it can also allow you to break apps unknowingly. For this reason, please read the following warnings:

WARNINGS:

1. Many running apps are required for functionality of the mobile device. Use of the *Force Stop* or *Uninstall* options may cause undesired results. *Force Stop* affect all processes and threads related to the app, and may also affect other apps which rely on any of the processes being closed.
2. Unintended use of *Clear data* or *Clear cache* options may destroy app configuration and affect app behavior.
3. Many installed apps are required for device functionality. Use of the *Force close* option may cause undesired results.

Privacy Audit

Privacy Audit helps you to maintain a more secure environment when using your mobile device. When you load this screen, all apps are scanned with regard to privacy settings. When the scan is complete, you will receive a breakdown of how your privacy may be affected by each installed app, based on the following criteria. You may need to scroll down to see the entire list. Here is a sample Privacy Audit. Categories which may appear on the Privacy Audit results are:

- **have network access** – These apps can access the Internet.
- **can read your personal info** – These apps can access your contacts, phone number and web history.
- **can access storage** – These apps can read and write files from your phone's memory.
- **can publish shortcuts to the main screen** – These apps can automatically create shortcuts on the main screen, a tactic often used by aggressive ad networks.
- **can block screen** – These apps can “steal your screen,” taking control of your phone away from you.
- **can cost you money** – These apps can send SMS messages and make calls.
- **can make calls** – These apps can make calls without user confirmation.
- **can track location** – These apps can access your location.
- **can access secure settings** – These apps can change your PINs and lock patterns.
- **can access calendar** – These apps can access your calendar.
- **can monitor calls** – These apps can record your calls.
- **can access text messages** – These apps can read your text messages.
- **can access accounts** – These apps can access your added system accounts. These accounts include (but are not limited to) your Google account.
- **can control hardware** – These apps can access your hardware, including (but not limited to) camera and NFC adapters.

Click on any category with apps listed to find out which apps are part of the list. Click on any app to find information about the app and about the resources it uses.

Malwarebytes Labs

While we do our best to protect you with our Malwarebytes protection products, we also make information available about the threat landscape, malware, and what we are doing here at Malwarebytes to make the computer world a safer place. **Malwarebytes Labs** has long been a staple on the Malwarebytes website, and it is now directly available from *Malwarebytes* in a format optimized for your mobile device. You can choose whether to read about what's happening in mobile devices, or computers as a whole.

News about malware threats can change rapidly, sometimes even while you're reading an article about it. For this reason, we have implemented pull-to-refresh on this screen. Simply swipe your finger downwards over the app to refresh your screen without leaving or reloading the page.

Settings

These options control many behavioral aspects of *Malwarebytes*. They are divided into two groups – Security settings and General settings. Here is more information.

Scanning

These settings allow you to enable/disable certain types of scans, and to schedule scans. Explanation of each setting is as follows:

- **Scan after reboot** – If checked, a full system scan will occur immediately after your device is rebooted. If unchecked, no scan will occur at that time.
- **Scan after update** – If checked, a full system scan will occur after each protection update. If unchecked, an update will not trigger a scan.
- **Use deep scanner during full scan** – If checked, full scans will use additional deep scanning rules. Scan times will increase, but will be able to detect additional items
- **Power saving scans** – If checked, *Malwarebytes* will not run a scheduled scan if your device battery is low or if the device is in power saving mode.
- **Perform scans during charge only** – If checked, *Malwarebytes* will only run scheduled scans when your device is charging.
- **Scheduled scans** – If checked, your device will be scanned automatically by *Malwarebytes* based on the following settings:
 - **Scan frequency** – Chooses whether scans will occur daily or weekly.
 - **The days of the week** – If *Scan Frequency* is set to Weekly, this option allows you to select which day(s) a scan should occur on.
 - **Time** – Select this to choose the exact time at which a scan will begin. Please note that if scans are scheduled to be run on multiple days, all scans will occur at the same time of day.

If **Scheduled scans** is unchecked (disabled), non-scheduled scans still occur on an on-demand basis.

Protection

These settings control whether many additional features offered by *Malwarebytes Premium* are enabled or disabled. Here is more detail on these settings.

Real-Time Protection (RTP)

When this setting is checked (enabled), *Malwarebytes Premium* and *Free+* version users are protected from threats and exploits that occur in real-time.

Protection includes:

- Additions and/or modifications to files on the file system
- Downloading of files from external sources
- Installation of downloaded files
- Execution of applications
- Insertion of SD memory cards

This notification is displayed when *Malwarebytes Premium* is used on Android 8 and Real-Time Protection is active. It prevents the background process from being terminated by Android.

 Malwarebytes

Crushes Malware. Restores Confiden..
Real time protection is active.



Anti-Ransomware protection (ARP)

Many components of ransomware can be detected and neutralized using Real-Time Protection, but there are other telltale signs that would not be caught by Real-Time methods because they appear innocent...on the surface. Premium users can enable this additional protection at the flick of a switch.

Scan Links Sent Via SMS

When this setting is checked (enabled), *Malwarebytes* will scan received SMS messages to assure that links in these messages do not contain phishing URLs. This type of malware is very prevalent in mobile devices. This setting may not be present if your device does not support SMS functionality.

SMS Device Control

This advanced security feature allows you to secure your phone remotely by sending SMS commands from another device. You can change the device password, activate a siren and display a message, or start ransomware remediation remotely. If your device supports SMS functionality, we highly recommend you activate this feature. Once enabled, you will be requested to enable Device Administrator (covered in the next section) if it is not enabled already, and to enter a six-digit password. You can then use your device even if it is blocked by some ransomware. Usage instructions for these commands are shown on the “How to use” section of the “SMS Device control” screen, and also shown here for reference. Please remember that these commands are meant to be executed **from** a second (remote) device. The commands will be executed **on** your device.

Show Usage Instructions

mb <password> how
mb <password> ?

Show a Message on your Screen

mb <password> display <message text>

Show Anti-Ransomware Notification with Remediation Instructions

mb <password> antiransomware
mb <password> arw

Change Password

mb <password> password <new password>

Lock your Screen

mb <password> lock

Activate Device Siren/Vibration

mb <password> alert

Other

These are miscellaneous settings primarily related to database updates and user notifications.

Device Administrator

This setting gives *Malwarebytes* full permissions on your device. This allows us to protect the user from ransomware, to enable real-time protection features and to safeguard against the possibility of malware uninstalling *Malwarebytes*. This setting is only available to Premium and Trial users.

Memory Caching

This setting is enabled by default, and allows *Malwarebytes* to use additional system resources to increase performance. Disabling this setting will reduce memory usage of the program, but will result in longer scan times. This setting is available for all users.

Database Updates

These settings determine how and when your device receives updates. A brief description of each setting is as follows.

- **Auto updates enabled** – Determines whether you receive threat protection updates automatically. If this setting is disabled, the setting for **Update frequency** is also disabled. **Please note** that this is a critical part of keeping your device protected.
- **Auto update Over Wi-Fi** – Allows you to specify whether you receive protection updates using Wi-Fi networks exclusively, or use a cellular network. Use of Wi-Fi allows you to reduce data usage.
- **Update frequency** – The interval between checks for protection updates. You may choose an interval of 1, 3 or 6 hours between checks. This setting is disabled if *Auto Updates Enabled* has been turned off.
- **Force Update** – A toaster message will inform you that the database is up to date, or that a database update is beginning. Please note that the date and time of the most recent update check will be shown here whether you actually download a database update. If your signatures are already current, there is no need to update again.

Notifications

This screen includes four settings which govern information provided by *Malwarebytes* during execution. Information pertaining to these settings is as follows:

- **Scan Result** – This setting controls whether scan results are displayed following execution of a scan when no malware was detected during the scan. *Malwarebytes* for Android will let you know when malware was detected. When no malware was detected, the choice is yours to make.
- **RTP icon** – This setting determines if Real Time Protection notifications are shown in the notification bar.
- **Database Updates** – This setting determines whether notifications will be displayed pertaining to database updates.
- **Issues** – Shows notifications related to device/program issues.

Help Us Anonymously

Checking this setting allows *Malwarebytes* to send usage characteristics for review. Usage characteristics is defined as:

- App Name and Version
- Device System Architecture (ARM, x86, etc.)
- Phone Locale
- OS Name (currently Android only)
- UUID (unique code associated with *Malwarebytes* installation on a specific device)
- Database Version
- Analytics will also be sent when malware has been detected as a result of real-time protection, an on-demand scan or a scheduled scan.

This information is sent five minutes after installation of *Malwarebytes*, and every six hours afterwards. If this option is turned off, App Name/Version and UUID will not be sent to Malwarebytes. All other information listed above will continue to be sent every six hours.

Share

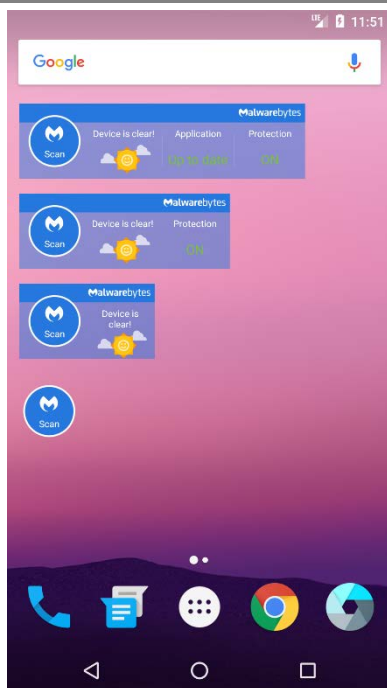
Pressing **Share** allows you to share *Malwarebytes* with one or more contacts. You can choose from the many Google services, email, or social networks which you are a member of. That varies from method to method and will not be shown here.

About

The **About** screen allows you to gather information about your *Malwarebytes* program, contact Malwarebytes and access a few surrounding your use of the software. Here are the details:

- **App version** is the version of *Malwarebytes*. This includes added information that is primarily used internally. The part you need to be concerned with the leftmost portion (v3.0.0).
- **Malware database** is the collection of threat signatures which keep you safe. It is updated on a regular basis.
- **Phishing database** is a database of known phishing methods that you may need protection against. It too is updated on a regular basis.
- **Help Center** gives you browser access to our Support Forums, downloadable user guides and more.
- **Send Feedback** allows you to tell us via email what you like and what you don't like. We want to know what you think!
- **License Agreement** launches a browser and connects to the Malwarebytes website, to allow viewing of the licensing agreement which governs use of all Malwarebytes products.
- **Privacy Policy** launches a browser and connects to the Malwarebytes website, to allow viewing of the Malwarebytes privacy policy.
- **Rate the App** connects you to the Google Play Store so that you can tell others what you think of *Malwarebytes*.

Widgets



You can create one or more Malwarebytes widgets on your Android Home screen. The *Malwarebytes* widget lets you see your device status at a glance. They can be configured to show 1-4 information items. After a widget has been created, press the widget and drag one of its edges to expand or compress it.

Scan Status

- **Scan** – Ready to scan your device
- **<x> Malware** – Scan running with progress shown in the ring; Number of threats shown as <x>
- **Scan Complete** – Scan complete with no threats detected
- **Check results** – When shown in orange, one or more PUPs were detected. Red indicates malware was detected

Device Status

- **Device is clear!** – Using a weather concept, clear skies ahead! Device settings are offering you maximum security.
- **Issues found!** – Cloudy skies and raindrops indicate settings which should be reviewed and corrected
- **Issues found!** – Cloudy skies and lightning means threats were detected.

Application Status

- **Up to date** – Your *Malwarebytes* database is up to date.
- **Update now** – Time to update your *Malwarebytes* database!

Protection Status

- **On** – Your device is being protected by Real-Time Protection
- **Turn on** – Real-Time Protection should be enabled on your device.