Malwarebytes for iOS
User Guide

Version 1.2.2

12 December 2018

Notices

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 thereto.

Table of Contents

Introduction

Welcome to *Malwarebytes for iOS ("Malwarebytes")*, our first entry into the Apple mobile device market. *Malwarebytes* protects you from malicious and suspicious web sites, unwanted phone calls and text messages, and web-based advertising. *Malwarebytes* is available with full functionality in Premium mode, and limited features in Free mode.

What's New

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

Improvements

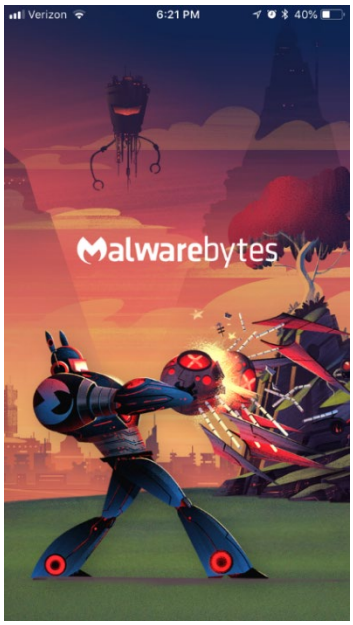
- Added ability to whitelist websites
- Added 3D Touch options to the Malwarebytes app icon
- Added tabs for reporting/blocking and allowing phone numbers

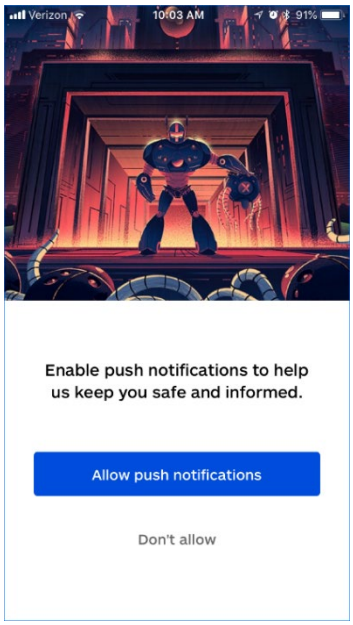
Stability/Issues Fixed

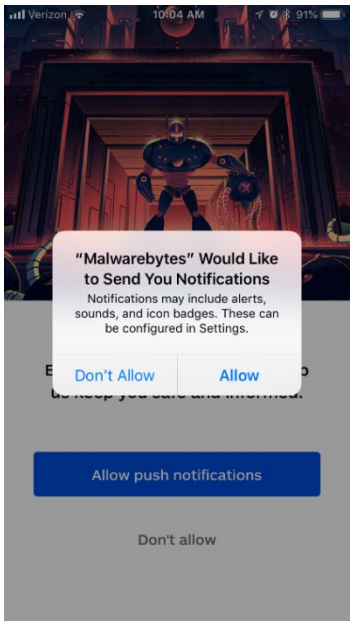
- Fixed a problem that caused calls from numbers in Contacts to be blocked
- Fixed minor issues

Quick Start

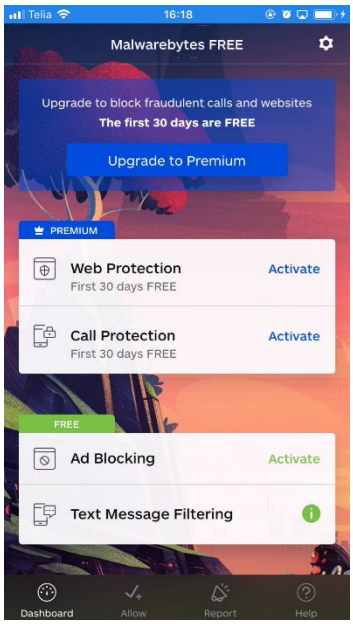
Let's walk through the steps needed to get you up and running. Don't be scared! After this one time, using *Malwarebytes* will be simple.



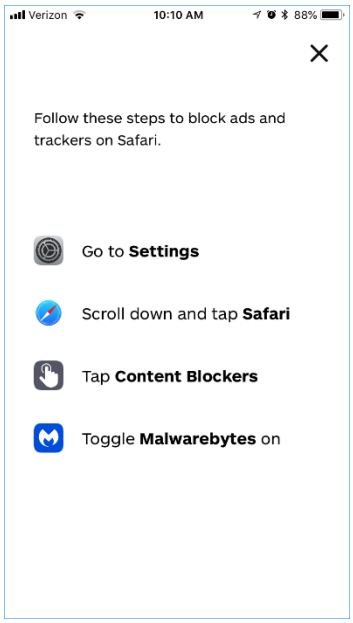




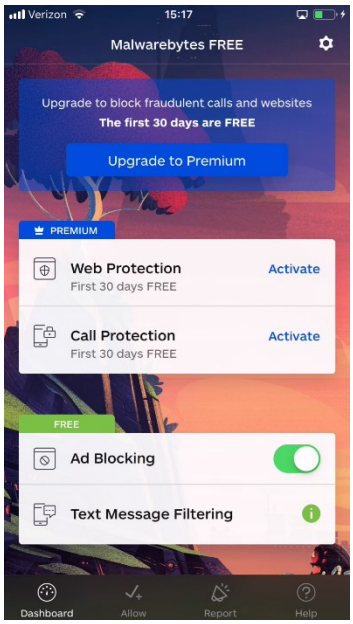
To the left is our hero, *Zero*. He appears throughout the app, to remind you we have your back.	We may need to let you know about something we think is important, so we ask your permission here.	iOS will also ask your permission. You can also enable this setting in **Settings ► Notifications**.



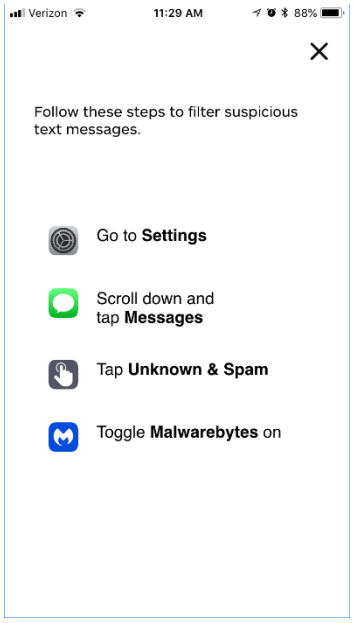
Tap **Activate** to turn on Ad Blocking.



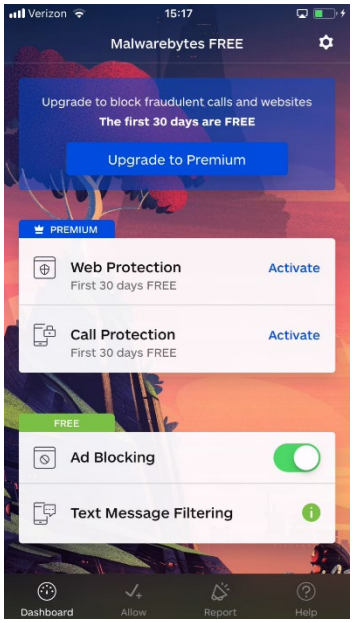
Open **Settings** to make the changes, then continue.



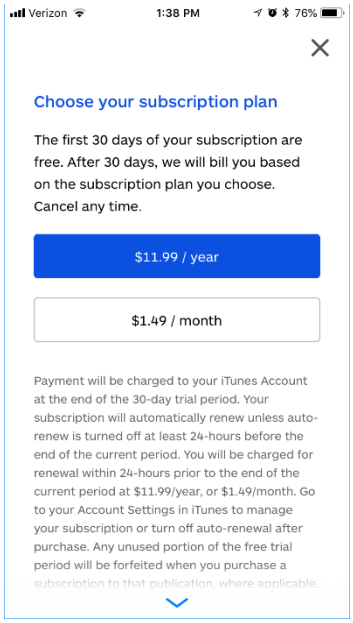
Ad Blocking is now enabled. Now we need to enable Text Message Filtering.



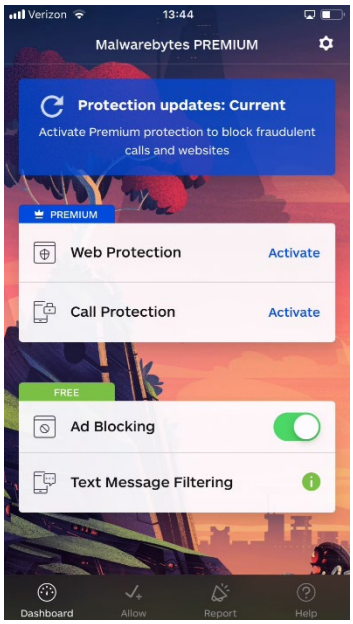
Open **Settings** to make the changes, then continue.



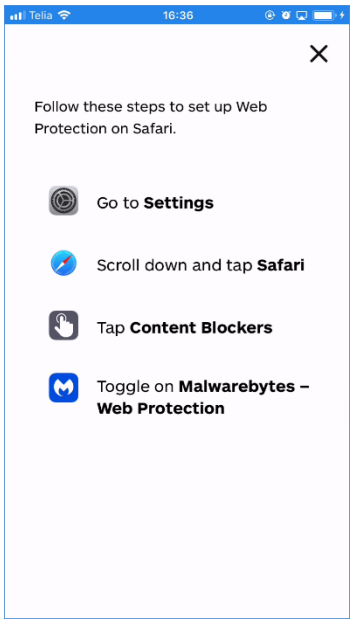
When you tap **Upgrade to Premium**, you will be sent to the Apple Store (shown in the next screen).



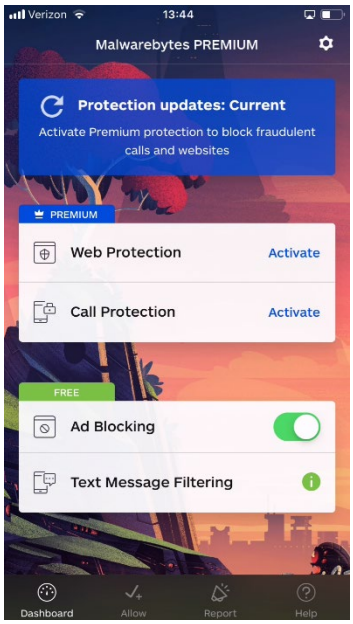
Choose the term of your Malwarebytes subscription. It will be billed to your Apple ID.



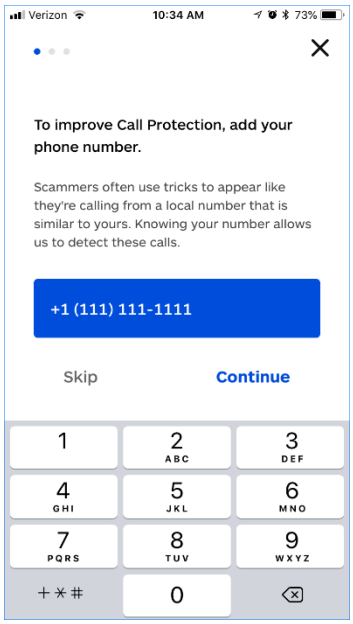
You are now ready to activate premium features. To enable Web Protection, tap **Activate**.



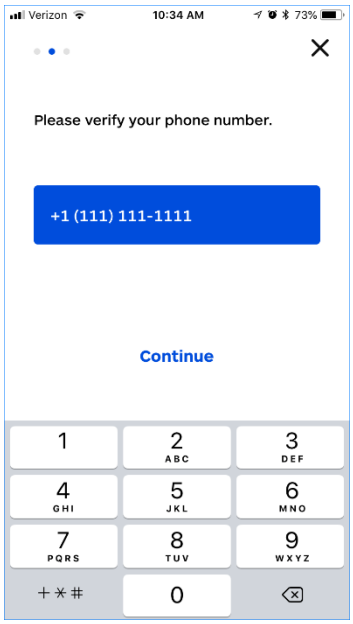
Open your phone's **Settings** app and follow these instructions.



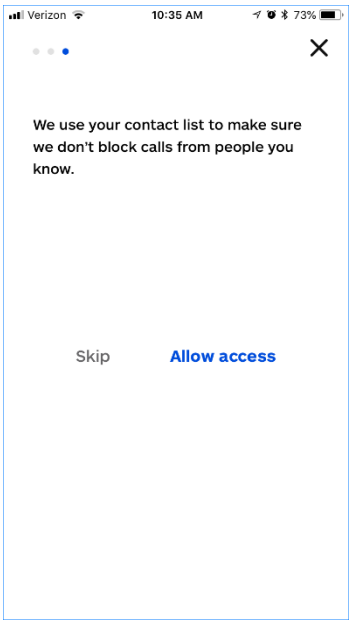
Tap **Activate** for Call Protection.

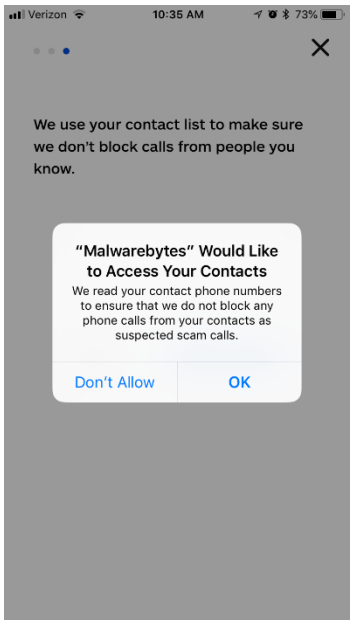


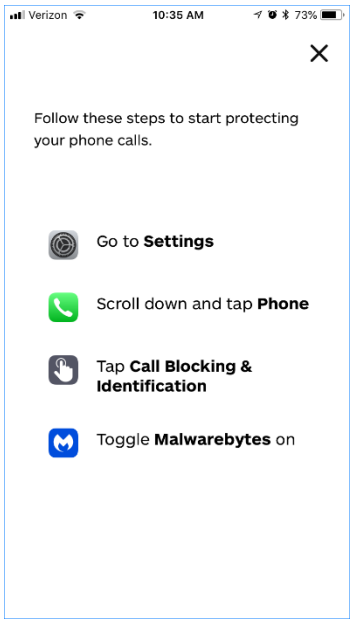
Enter your phone number. This protects you against *neighbor spoofing*. More on this later. Tap **Continue** when done.



Please re-enter your phone number, then tap **Continue**.







We use your Contact List so you can receive calls from these people and don't have to enter them all in yourself.	We do need to ask your permission though!	These are the changes needed. Open **Settings** to make the changes.

Free vs. Premium

Malwarebytes can be used as a free app or as a paid (Premium) app. The Premium app offers more features, and is available on a monthly or annual subscription basis. If you purchase a Premium subscription, the first month is free (terms available at time of purchase). Following are the features which *Malwarebytes* provides.

All Users

- **Ad Blocking –** This feature prevents display of web-based advertising when you are using a Safari browser. This feature is available *only* for the Safari browser at the present time. This feature requires a change to iOS settings.
- **Text Message Filtering –** This feature analyzes text messages and sends those considered suspicious to a junk tab. Messages categorized as suspicious may also be sent to Malwarebytes servers for analysis, so that we can provide better protection for all users. Transmission to Malwarebytes is controlled by a setting within *Malwarebytes* (to be discussed later). This feature requires a change to iOS settings.

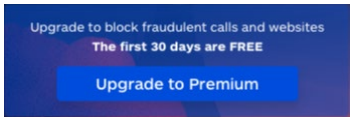
Premium Users only

- **Web Protection –** This feature utilizes Malwarebytes' comprehensive database of suspicious and malicious websites to assure you do not unknowingly become a victim. This feature is supported for all web browsers.
- **Call Protection –** This feature uses your Contacts list and opt-in authorizations to control your exposure to scammers, spammers and telemarketers. This feature requires a change to iOS settings.

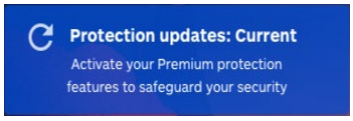
When you first launch *Malwarebytes*, you will be in free mode. You may upgrade to a Premium subscription at any time, by making an in-app purchase through Apple's App Store. Premium users who have deleted/reinstalled or moved to a new device will appear as Free users until they restore their subscription.

Dashboard

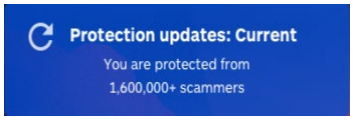
This screen shows the program's features and their status (activated/enabled/disabled). Premium features are available only to users who have purchased a Premium subscription, while Free features are available to all users. The top third of the screen shows status, which is described here.



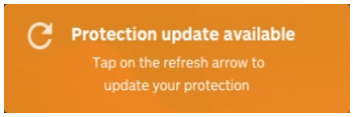
Encouragement for Free users to get maximum protection by purchase of a Premium subscription.



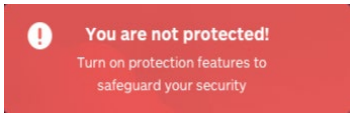
Malwarebytes protection databases are up to date. Activate Premium mode for maximum advantage.



Malwarebytes protection databases are up to date, and Premium features are protecting you now.



Malwarebytes has been unable to update protection databases. Tap refresh to try again. This is dependent on Internet access.

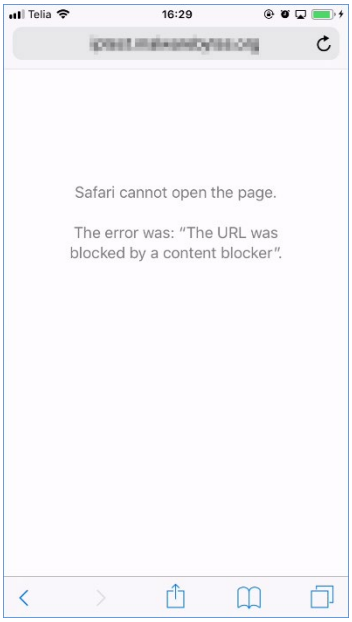


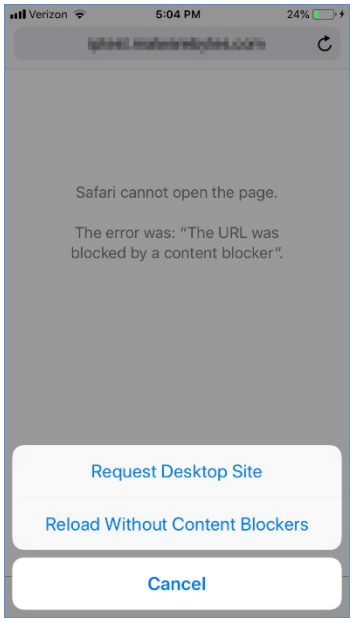
Malwarebytes protection features have been activated, but one or more has been disabled. Enable all features to return to normal status.

The remainder of the Dashboard controls the features of *Malwarebytes*, separated into Premium features and Free features. The Quick Start section of this guide helped you enable the features on your device. We will now give you more detail about each feature.

Web Protection

Web Protection stops you from accidentally visiting malicious websites known to contain phishing scams, malicious content, or other online threats. Web Protection only works with the Safari browser. If you open a link to a malicious site, *Malwarebytes* will prevent the website from loading. If you wish to view the site, you can temporarily disable Web Protection. Here's how to do that.



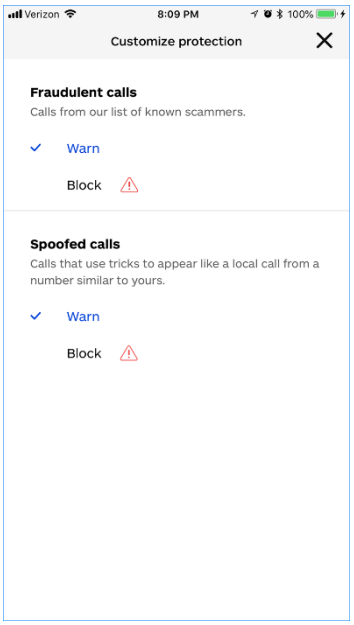


Safari is letting you know that we blocked access to a website.	If you want to visit the site, tap and hold the ↻ icon in the upper right, then tap **Reload without content blockers**.

If you trust that the website is not malicious, you can also add it to your Web Allow List. Steps on how to do this are explained in the Allow section of this guide.!

Call Protection

Call Protection warns you when an incoming call is from a suspected scammer. It works by referencing a list of known scammers (maintained by Malwarebytes), including numbers reported by users like you. Call Protection also catches scam calls that use tricks to appear like they're calling from a number similar to yours (*neighbor spoofing*). Your Contacts are never blocked, so you won't miss calls from your friends. We will ask for your phone number as well as access to your Contacts, and you must allow access to the list if you want to exempt them from Call Protection. In addition to your Contacts, you may manually add phone numbers to be automatically allowed to contact you. When a fraudulent call comes in, you'll see "Malwarebytes: Suspected Scammer" as part of the caller ID information for neighbor spoofs, or "Malwarebytes: Known Scammer" for numbers in our database. You may also report fraudulent phone numbers to Malwarebytes through your app. This allows us to analyze its usage, and allows Call Protection to automatically block incoming calls on your device that originate from that number.



Call Protection can be used in either *Warn* or *Block* mode. In Warn mode (the default), you will see all incoming calls, but a scam call will be labeled as a *suspected* or *known scammer*. The call will appear in your call history, and you will receive a voicemail, if they left one.

In Block mode, you will not see that a call came in at all. The phone will not ring, and there will be nothing left in your call history, or possibly voicemail (carrier-dependent). Be aware that Malwarebytes cannot see when calls are warned about or blocked, because Apple does not allow apps to see that information. If a call is blocked, there will be no way to see anything about the call.

A word of warning about the Block setting…because you will not know anything about incoming calls from numbers that were blocked, you may miss a legitimate call if you flagged the number incorrectly. Please consider using Warn mode instead.

Call Protection only works on iPhones. Although your iPhone can forward calls to an iPad, Call Protection will not work for calls forwarded to an iPad.

Ad Blocking

Ad Blocking prevents your Safari browser from loading ads. When web pages are laid out, they use code to signify where content will be placed, and what will be placed there. Based on this, we detect and block advertising content. It also blocks ad trackers, which monitor your online behavior. Ad Blocking also allows web pages to load faster. Ad Blocking uses a content filter in Safari. Ads and trackers will simply be blocked, with no visual indicator that anything was blocked. Malwarebytes cannot see what sites you visited or what was blocked.

Text Message Filtering

Text Message Filtering sends suspicious text messages to a junk tab in your Messages app. It works by comparing the sender's phone number to a list of known scammers and detecting phishing links within the message. Texts from your Contacts are never filtered, so you don't have to worry about missing messages from your friends. Texts from unknown senders will be sent to a Malwarebytes server for analysis. We take your privacy very seriously. For more information about what information we handle during this process and how we protect it, see:

https://links.malwarebytes.com/link/ios_security_of_text_message_filtering

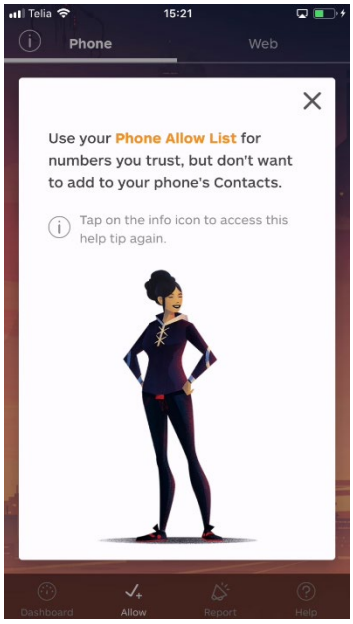
You may also report fraudulent phone numbers to Malwarebytes through your app. This allows us to analyze its usage, and allows Text Message Filtering to automatically block incoming messages on your device that originate from that number.

Allow

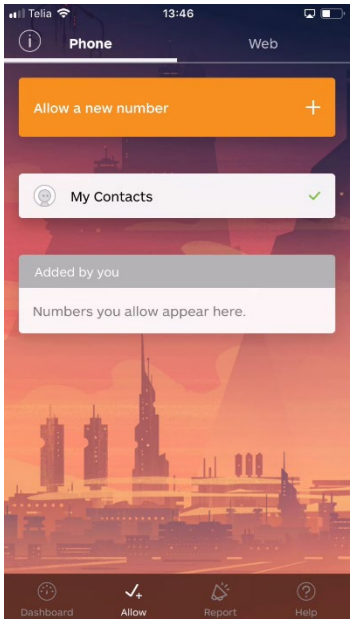
The Allow screen provides you the ability to prevent *Malwarebytes* from blocking specific phone numbers or websites that you trust. You can toggle between the Phone and Web allow list using the menu at the top of the screen. Details on how to customize your protection for each feature follow.

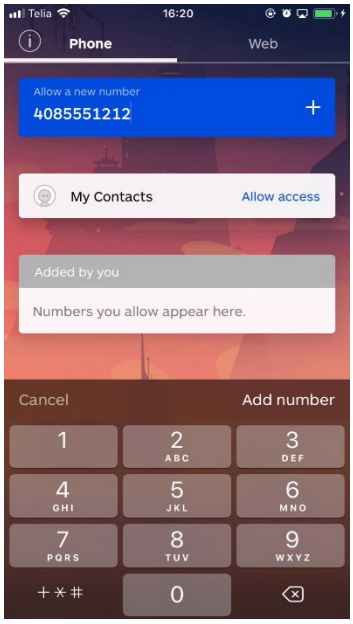
Using the Phone Allow List

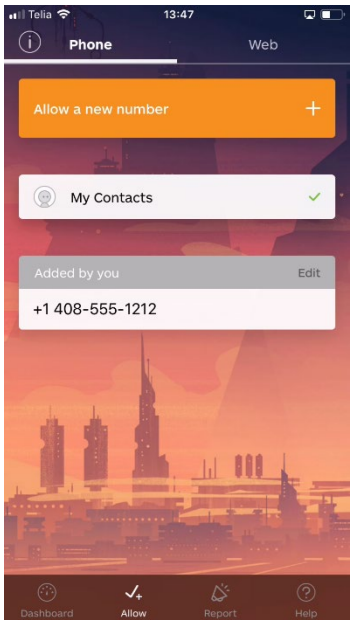
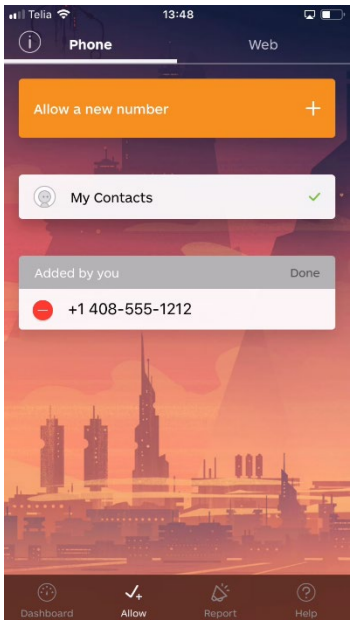
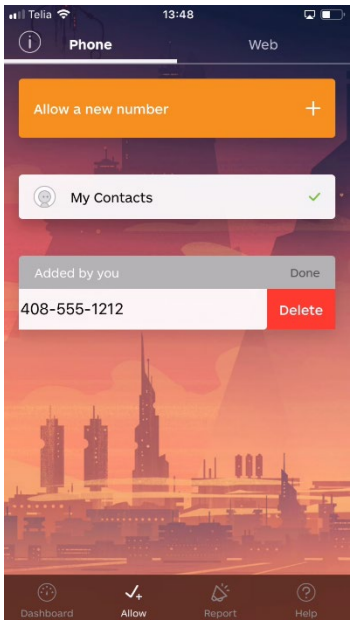
In addition to the Phone app's *Share Contacts* button and the 3D Touch button, you can also add phone numbers to your Phone Allow List directly from the *Settings* screen. Here's how…



The first time you access the Phone Allow List, this screen appears to explain the feature.	Initially, the Phone Allow List contains only your Contacts. Tap **Allow a new number** to add to the list.	Enter the phone number in the blue bar, then tap **Add Number**. Please note: Only US and Canadian phone numbers can be entered at the present time.

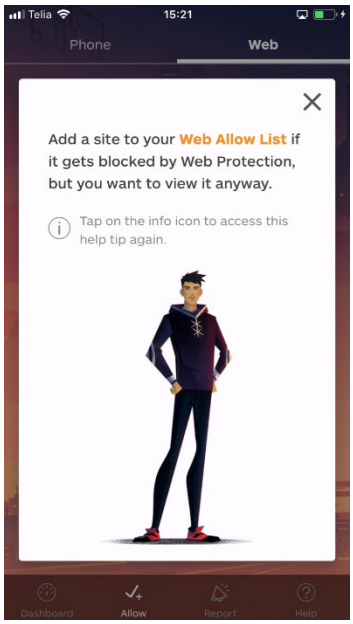




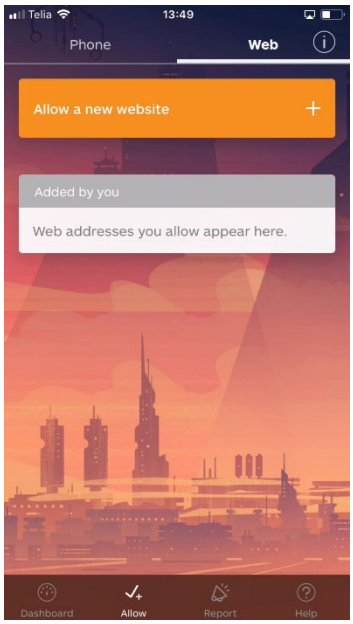
		
The number is now shown in the lower section. To delete a number, tap **Edit**.	Tap the number (or numbers) you wish to delete.	Tap **Delete** to confirm that you wish to remove the number(s) from your list.

Using the Web Allow List

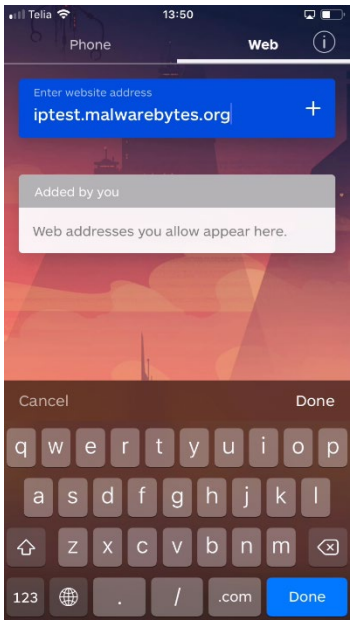
You can also add, edit or delete website URLs from your Web Allow List directly from the Settings screen. It's as easy as this!



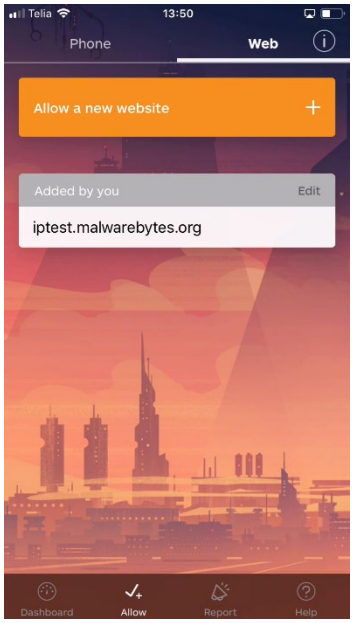
The first time you access the Web Allow List, this screen appears to explain the feature.



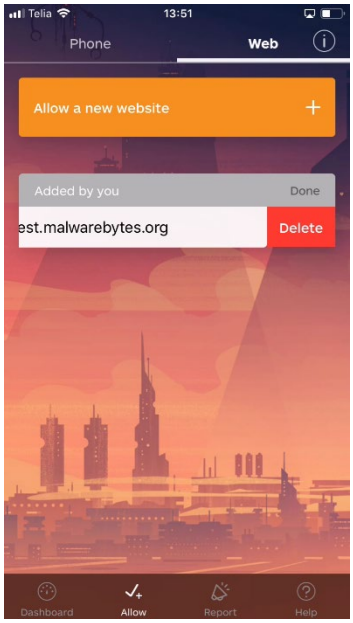
The Web Allow List looks like this before any sites have been added.



Tap **Allow a new website** and type in its URL, as shown here.



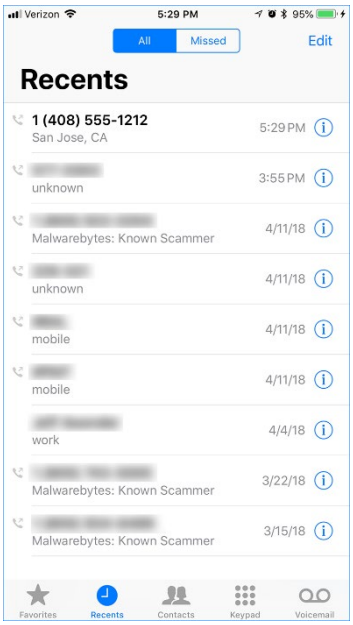
The website will now appear in your Web Allow List.



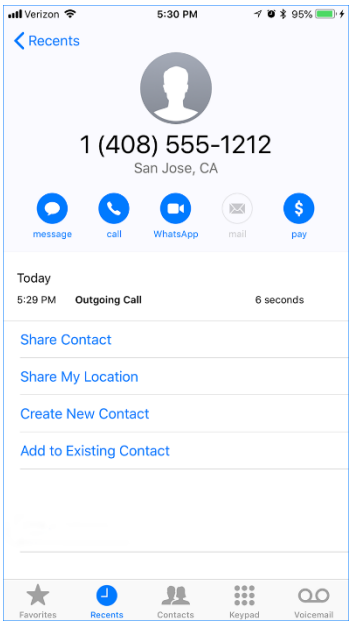
To delete a site from the list, tap **Edit** followed by **Delete**.

Allow Phone Numbers via Share Contacts

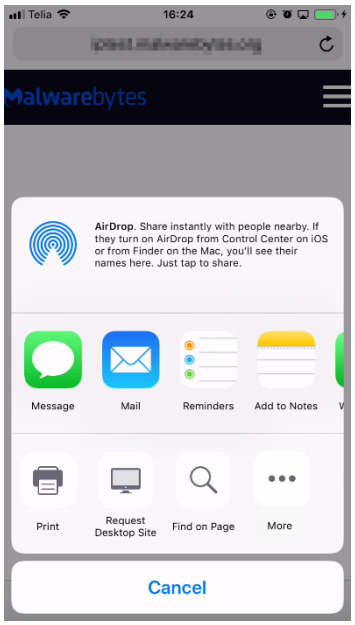
Malwarebytes integrates with your Phone app's Recents screen to populate the Phone Allow List as well as to Report a fraudulent number. A shortcut exists to help you do this more quickly, and we will show it to you here.



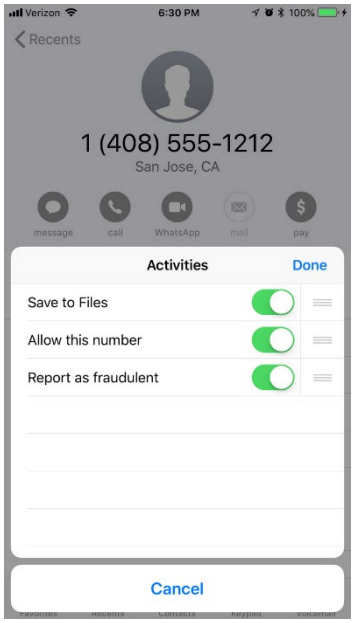
Tap the ⓘ icon to select a phone number. A new screen will be displayed with options.



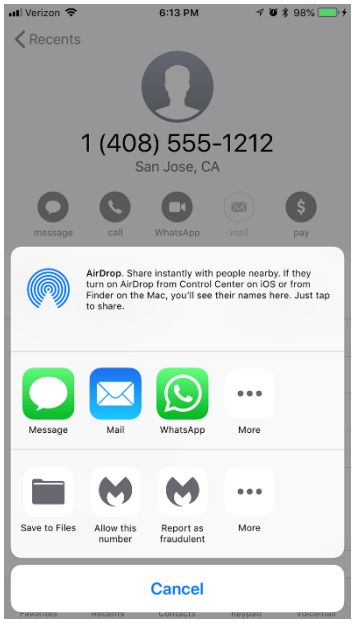
Tap **Share Contact**.



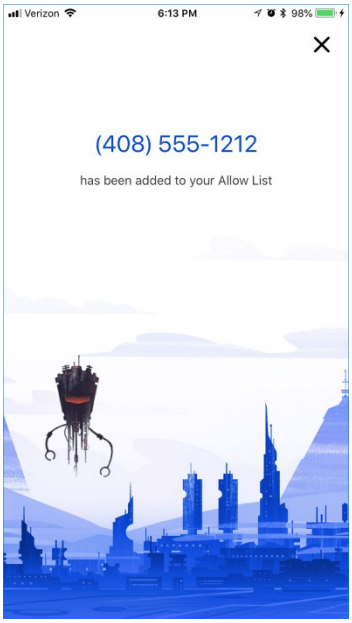
Tap **More** (on the bottom row) to see the Activities screen as shown in the next panel.



After you enable **Allow this number** and **Report as fraudulent**, you won't see this ever again!



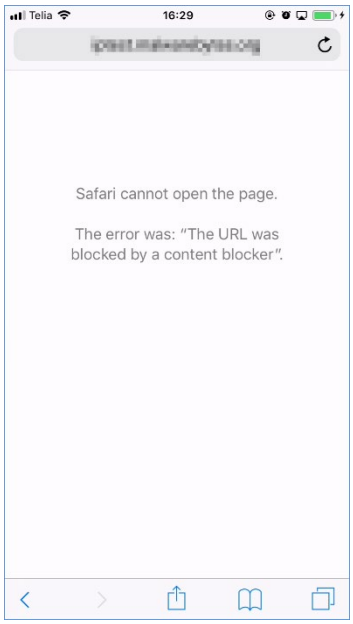
You will see this instead. Only one tap is needed now.



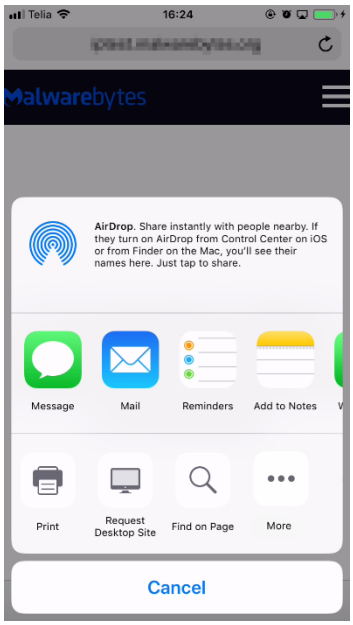
This is what you will see after adding a number to your Phone Allow List.

Allow Websites via Share

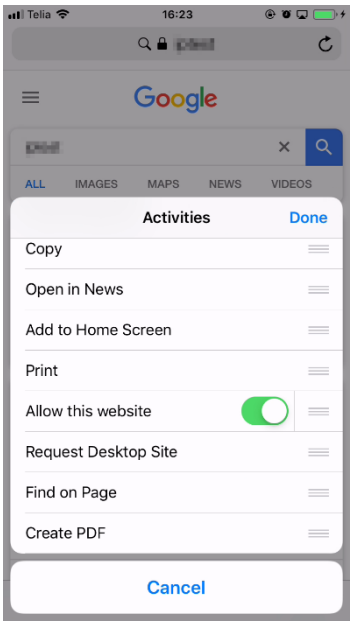
You can quickly allow access to a website that *Malwarebytes* has blocked using the Share feature on your phone. These steps will guide you through the process.



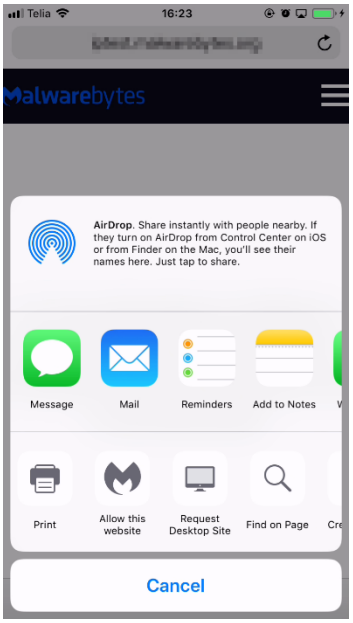
Tap the icon to open the share menu with additional options.



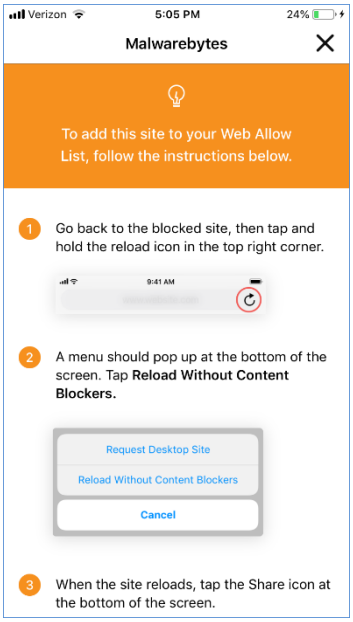
Tap **More** (on the bottom row) to see the Activities screen as shown in the next panel.



Enable **Allow this website**. You only need to do this once.



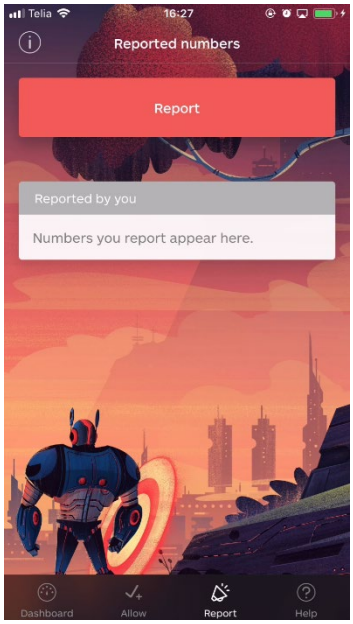
You will see this instead. Now you can quickly add to the Web Allow List. Tap **Allow this website.**



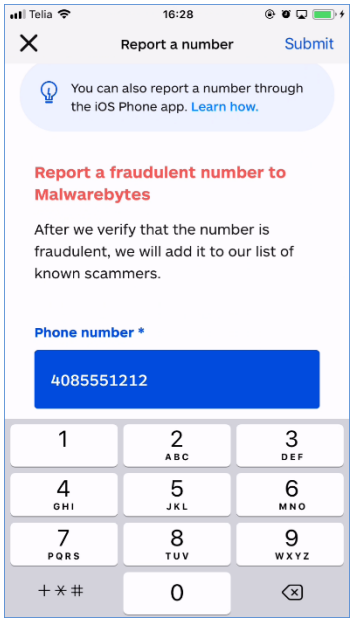
If you are allowing a site that was blocked by *Malwarebytes*, you must perform the additional steps shown. Afterwards, *Malwarebytes* will no longer block the site.

Report

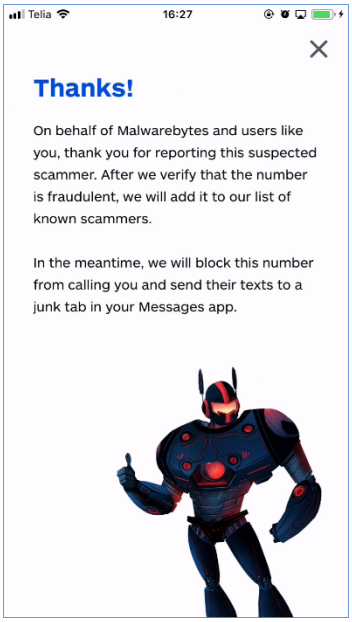
If you suspect a number is a scammer, you can report it to us using the **Report** tab. Numbers that you send to use will have their text messages automatically filtered. After you report a number, we will verify if it is indeed a scammer, and if so we will add the number you shared with us to our list of known scammers. Your submissions help us provide better protection for everyone!



Tap **Report** to submit a new suspected spam caller for review.



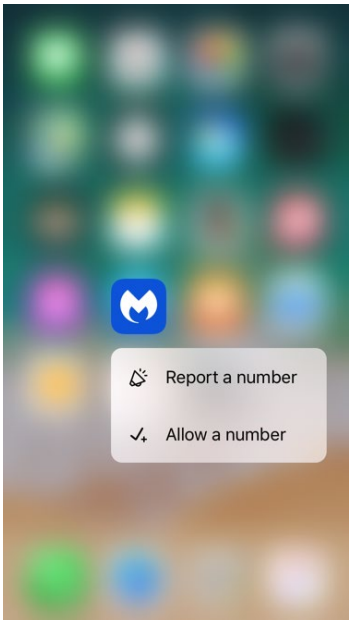
Enable **Allow this website**. You only need to do this once.



Once you submit the number, we will review it to confirm it is fraudulent.

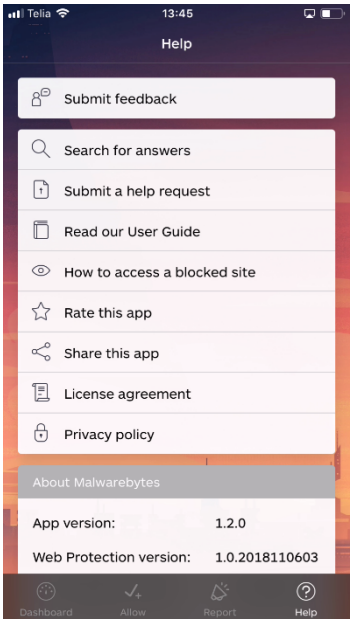
3D Touch

You can use your iPhone's 3D Touch feature to allow or report numbers. Press firmly on the *Malwarebytes* icon on your phone to open the 3D Touch Menu. From the menu, tap either **Report a number** or **Allow a number** to open the corresponding page.



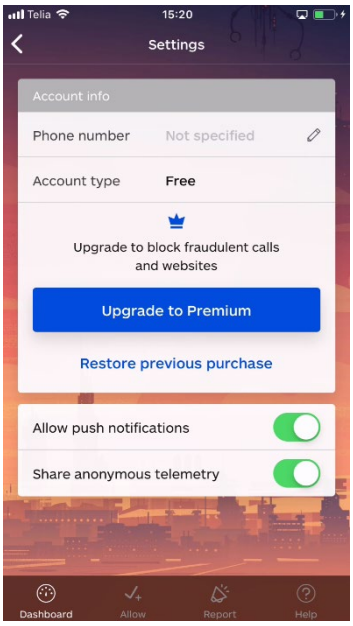
Help

The Help screen is designed to answers your questions about Malwarebytes and the *Malwarebytes* app, and to give you a chance to provide feedback. Specific options available here include:



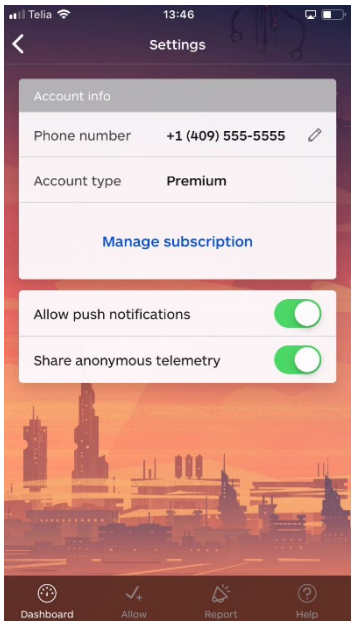
- **Submit feedback –** Please take our survey and tell us what you think.
- **Search for answers –** This link opens your Safari browser and takes you to our Customer Success Knowledgebase, where you can find answers to the top questions being asked.
- **Submit a help request –** If you can't find an answer, email us!
- **Read our User Guide –** This guide! If you find a problem, please let us know!
- **Rate this app –** Rate this app in the Apple Store. Your voice counts.
- **Share this app –** If you like it, share it with your friends.
- **License agreement –** There's no escaping these, and this link takes you to the Malwarebytes website to read ours.
- **Privacy policy –** This details what information we may collect, and why we do it. While the policy is detailed, it is also easy to read.
- **App version –** The *Malwarebytes* version installed on your device.
- **Call Protection version –** This is a database of known spammers and scammers. *Malwarebytes* will use this database to block incoming calls from phone numbers in this database.
- **Ad Tracker version –** This is a database of websites who inject advertising into web pages opened in your Safari browser. This allows us to block the ads and trackers which those websites use.

Settings



Shown here are the Settings screens, Free mode to the left, and Premium mode to the right. You can access the Settings screen by tapping the ⚙ icon. You will notice differences in the contents of the top section of the screen. This is to demonstrate the variations of the display based on Free vs. Premium modes.

The bottom section contains settings that are universal.



Following is more detailed information for each of these settings.

- **Phone number –** You can enter, edit or view the phone number you have entered. This is also used as a basis for Call Protection, as some scams use *neighbor spoofing* – phone numbers designed to look like a local number.
- **Account type –** Quickly informs you the type of account (Free or Premium) that you have for your app.
- **Upgrade to Premium** (Free users only) **–** Tap this button to purchase a Premium subscription through Apple's App Store.
- **Restore previous purchase –** This link allows Premium users to reconnect with their Premium subscription after (a) deleting and reinstalling *Malwarebytes* on the same device, or (b) installing *Malwarebytes* on a different device, to restore their Premium subscription on the current device. **Please note:** Subscriptions are linked to the Apple ID they were purchased with, and can only be used on devices signed in to that Apple ID. Subscriptions cannot be shared using Apple's Family Sharing plans.
- **Manage subscription** (Premium users only) **–** This link allows a Premium user to manage his subscription, such as cancelling the subscription or managing payment information. Please note that subscription management is handled by Apple.
- **Allow push notifications –** Allows you to enable or disable push notifications (notifications that *Malwarebytes* is allowed to display in the *iOS Notification Center*).
  Share anonymous telemetry – *Malwarebytes* will periodically send anonymized information about your device, such as the iOS version in use, and the installed *Malwarebytes* version. This helps us better understand our users. You can turn this setting off if you choose.