WEBROOT®
by opentext™

Mobile Security for iPhone
User Guide

Table of Contents

Notices

Mobile Security for iPhone User Guide revision Wednesday, September 25, 2024.

Information in this document is for the following product:

- Webroot Mobile Security for iPhone

One or more patents may cover this product. For more information, please visit https://www.opentext.com/patents.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Open Text.

Mobile Security for iOS overview

Webroot Mobile Security for iOS is available when you purchase Webroot Internet Security Plus, Webroot Internet Security Complete, or Webroot Premium packages.

Just as Webroot provides protection for Windows and Mac computers, Webroot Mobile Security for iOS delivers protection against viruses, spyware, and other online threats. Once installed, Webroot Mobile Security scans your device and informs you about vulnerabilities and weakness in your device protection, such as unsecured Wi-Fi networks, missing layers of passcode and biometrics security, and more. While shopping and banking online, Webroot protects your privacy and your data by blocking phishing sites, spam sites, malware sites, and other malicious activities.

The Webroot Mobile Security license is transferable for upgrades or changed devices.

Installing Webroot Mobile Security on your iOS device

Before you install Webroot Mobile Security for iOS, confirm that your device matches the system requirements at https://www.webroot.com/us/en/support/system-requirements.

An active internet connection is required.

To install Webroot Mobile Security on your iOS device:

1. From the App Store, download and install the Webroot Mobile Security app.
2. Tap the Webroot app icon to launch the app.
3. If you upgraded from a previous version, tap **Log In** and use your existing credentials.
4. For new users, under **Create Account**, enter your product keycode.
    - The keycode can be found in the receipt email for online purchases, or on a card for retail purchases and will look something like this: **WSAM-ZZZZ-0000-YYYY-1111**
    - If you don’t have a keycode, tap **Trial Here** to create an account for a trial period.
5. Enter your email address or phone number to be used as your username.
6. Create a password, following the strong password guidelines that are displayed.
7. To review how Webroot processes your personal data, tap **Privacy Policy**.
8. Tap **Create Account**. The **Webroot Subscription Terms** screen appears.
9. Tap **Solution Agreement**, read the terms, and tap **AGREE** to continue.

10. On the welcome screen, tap **Go**.

11. When prompted, tap **Allow** to grant the permissions necessary for the app to function properly.

Managing your account

To view and manage your account information, tap **My Profile**. From the **My Profile** screen, you can view information about your current plan, such as your plan details, keycodes associated with your account, account credentials, and app version. You can also manage your subscription and activate new keycodes.

To upgrade your current plan:

1. On the Dashboard screen, tap **My Profile**.
2. If you have a paid subscription plan, tap **UPGRADE OR RENEW**. If you have a trial plan, tap **UPGRADE**. The Webroot **Renew / Upgrade** webpage opens in your browser.
3. On the **Renew / Upgrade** webpage, enter your keycode in the **Keycode** box.
   - You can find the keycode in the receipt email for online purchases, or on a card for retail purchases. It will look something like this: **F123-ABAB-XY12-1234-5678**
4. Tap **Confirm and Continue**.
5. Follow the on-screen instructions to complete your renewal or upgrade.

To activate a new keycode:

1. On the Dashboard screen, tap **My Profile**.
2. Tap **ACTIVATE NEW KEYCODE**.

3. On the **Add Keycode** page that opens, enter your new keycode in the **Add Keycode** box. Then, on the **My Profile** screen, your new keycode is highlighted and appears at the top of your **Keycode(s)** list.

Managing threats with Mobile Security for iOS

After installation, Mobile Security for iOS immediately runs a first-time scan of the device. Once the scan is complete it will show a **Safe** or **Attention Needed** status.

After the initial scan, the app notifies you when it detects an online security risk.

You can respond in several ways:

- **Unblock** (not recommended) unblocks the alert and continues to the high-risk website. Only unblock sites if you are familiar with them or if you have verified that they are not threatening to your personal information or security.
- **Request a Review** sends a request to Webroot's threat experts to review and verify the site.
- **Go Back** redirects you to the last visited page, or a safe blank page to continue browsing. This is the best option for websites that you have not visited before.

Using Webroot for Safari

Webroot Mobile Security uses a plugin that provides additional protection while using the Safari browser. Webroot for Safari checks websites for malicious or suspicious content and warns you before you visit them.

Note that this feature is only available on devices that are running iOS 15 and above.

To enable Webroot for Safari, from the Webroot Mobile Security Dashboard, tap **Webroot for Safari** and follow the on-screen instructions.

When Webroot for Safari detects a high risk website, you can respond in one of the following ways:

- **Unblock** (not recommended) unblocks the alert and continues to the high-risk website. Only unblock sites if you are familiar with them or if you have verified that they are not threatening to your personal information or security.

- **Request a Review** sends a request to Webroot’s threat experts to review and verify the site.

- **Go Back** redirects you to the last visited page, or a safe blank page to continue browsing. This is the best option for websites that you have not visited before.

Webroot for Safari also annotates search results so that you know which links are safe before clicking on them.

To search using annotations:

1. From the Webroot Mobile Security Dashboard, tap **Webroot for Safari**.

2. If you have not enabled Webroot for Safari, follow the on-screen instructions to enable it.

3. Run an internet query, such as a Google search. Webroot for Safari displays icons and

messages that give you safety information about each website returned as a result of the search.

With Webroot for Safari, an icon accompanies each website listed in your returned search results, indicating the safety level of each website. The following table describes those icons and their meaning.

Icon	Description
✓	Trustworthy. This website is safe to visit.
⊖	Caution. This website might contain content that could affect your online security.
❗	Malicious. This website contains malware or other security risks.

Password management with LastPass

With LastPass, you can create and save strong passwords in an encrypted vault using the Carbonite/Webroot My Account portal. Once you create your LastPass account and start saving your credentials, you will be able to automatically log in to your favorite websites and auto-fill web forms. This saves you the hassle of manually entering your credentials, personal information, and credit card numbers.

LastPass Password Manager is included with your paid subscription of Webroot Mobile Security and is available only for Internet Security Plus and above licenses. If your subscription does not include Password Manager, contact Webroot Support or your administrator to upgrade your subscription.

To start using LastPass:

1. From the Webroot Mobile Security Dashboard, tap **Password Manager**.
2. If you are a new user and do not have an account with **My Account**:
    a. Tap **Get keycode** and **Copy** an available keycode.
    b. Tap **Go to My Account Portal**. In the browser tab that opens, enter the required information, including the keycode that you copied.
3. If you are an existing **My Account** user, but do not have a LastPass account:
    a. Tap **Go to My Account Portal**.
    b. Follow the steps on the **My Account** page to log in.
    c. On the navigation pane, go to the **Downloads** tab.

   d. Scroll down to **LastPass Password Manager** and click **Account Setup**.

   e. Follow the steps to sign up for a LastPass account.

4. If you already have a LastPass account:

   a. Tap **Open LastPass App**. The app opens in the App Store.

   b. Tap **Install**. When it has finished installing, open the LastPass Password Manager app and log in.

For more information about LastPass, see the LastPass Reference Guide.

Viewing your Activity Report

Activity Report allows you to see how Webroot Mobile Security is protecting your device from malicious websites. You can view your device's activity from the last 30 days and resolve any detected threats.

Note that Activity Report is included with your subscription of Webroot Mobile Security and is available only for Internet Security Complete and above licenses. If your subscription does not include Activity Report, contact Webroot Support or your administrator to upgrade your subscription.

From the Webroot Mobile Security Dashboard, tap **Activity Report** to view a summary of website threats that Webroot Mobile Security detected over the last 30 days. This summary includes the total number of websites visited and the number of new threats detected, as well as websites that are blocked, dismissed, and under review.

If you trust a website that Webroot Mobile Security flagged as a threat, or no longer want to see it listed, you can remove it from your Activity Details list.

To remove a website from your Activity Details list:

1. From the Activity Summary Report page, tap the **VIEW DETAILS** button. The **Activity Details** page displays.

2. To only display previously dismissed website threats, turn on the **Show only dismissed threats** switch.

3. Tap the **Delete** button 🗑 next to a website from the list. Tap **CONFIRM** to remove that website from the Activity Details list. Note that this only removes the website from appearing in your Activity Details list and does not change the threat status of that website.

Scanning recommendations

If Webroot Mobile Security detects any potential risks during a scan, the Security Recommendations screen will appear. You can tap **IGNORE** to dismiss each Security Recommendation, or click the arrow to learn more about each type of risk.

For optimal security and performance, we recommend that you consider the following potential security risks and best practices when running a scan on your iOS device:

- iOS updates
- Wi-Fi security tips
- Passcode and biometrics security
- Potential jailbreaking vulnerabilities

iOS updates

Operating software releases include the latest features and security updates that patch various vulnerabilities to protect your device. Plus, newer apps might only work with the latest iOS version. We strongly recommend you upgrade to the latest version when it is released.

Recommendation:

It is a best practice to upgrade to the latest version when it is released. You can do this manually, or turn on automatic updates.

To check for the latest iOS version on your device:

- Go to **Settings** > **General** > **Software Update**.
  - This screen shows the currently installed version of iOS and whether an update is available.

To turn automatic updates on or off:

1. Go to **Settings** > **General** > **Software Update** > **Automatic Updates**.
2. Turn the **Download iOS Updates** switch on or off.
3. Turn the **Install iOS Updates** switch on or off.

Wi-Fi security tips

We strongly recommend that you do not disable any device security settings before using a Wi-Fi network. This might disable device authentication and encryption and it would allow others access to your network and shared resources and make you more susceptible to malware and ransomware attacks.

Recommendation:

- If possible, always use a secured network.
- If you must use a Wi-Fi network, use a WPA2/WPA3 protocol to configure your settings.
- Install the Webroot WiFi Security & VPN app when using a Public Wi-Fi network.

Passcode and biometrics security

To secure your device:

- Set a passcode for your device. This turns on data protection, which encrypts your data.
- Enable **Face ID**.
- Enable **Touch ID**.

Note: Apps that support Touch ID also automatically support Face ID.

Recommendation:

A strong passcode, in combination with the biometrics security offered by Face ID and Touch ID, is the best way to secure your device and protect the information on it.

Potential jailbreaking vulnerabilities

Jailbreaking is an unauthorized modification that bypasses security features and can cause numerous issues to your device. This exposes your device to potential vulnerabilities and security threats.

Recommendation:

If you have a jailbroken device, perform a factory reset. This erases all data and apps on your device. The reset restores your device to its original factory settings.

Technical support

Webroot offers a variety of support options. You can do any of the following:

- Is your Webroot subscription through Best Buy? Click here for additional support options.
- Submit a help request.
- Look for the answer in our online documentation.
- Look for the answer in our knowledgebase and FAQs.
- Connect to the Webroot Community.