



Web Threat Shield User Guide

Copyright

Web Threat Shield User Guide revision Friday, June 7, 2024

Information in this document is for the following product:

- Web Threat Shield

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.

© 2004-2024 Open Text. All rights reserved.

Table of Contents

- Web Threat Shield User Guide overview 2
- Downloading and installing Web Threat Shield 3
- Understanding filter results 5
 - Running an internet search 5
 - Visiting a website 7
 - Encountering a block page 10
- Requesting a website review 11
- Technical Support 12

Web Threat Shield User Guide overview

Webroot® Web Threat Shield offers top-of-the-line defense against cybercrime while browsing the internet. It warns about unsafe websites before you visit them, and automatically blocks malicious ones trying to install viruses and malware on your computer.

Web Threat Shield also provides up-to-the-minute data about website reputations and real-time protection against phishing sites.

Web Threat Shield is included with your subscription of Webroot SecureAnywhere® Antivirus, Webroot SecureAnywhere® Internet Security Plus, or Webroot SecureAnywhere® Internet Security Complete.

If you install Webroot SecureAnywhere® on a Windows device, your browsers will ask you to authorize Web Threat Shield the next time you open them. If you decline authorization after installing Webroot SecureAnywhere®, or if you are using a Mac or Chromebook™ device, you will have to manually add Web Threat Shield to your browsers. See [Downloading and installing Web Threat Shield](#).

After downloading and installing Web Threat Shield, see the following topics:

- [Understanding filter results](#)
 - [Requesting a website review](#)
-

Downloading and installing Web Threat Shield

If you are using a Mac or Chromebook device, or if you declined installing the Web Threat Shield browser extension when you first downloaded Webroot SecureAnywhere, you will have to manually download and install Web Threat Shield.

To manually download and install Web Threat Shield:

1. [Purchase a SecureAnywhere keycode](#) if you don't already have one.

Note: You can purchase your keycode directly from [Webroot.com](https://www.webroot.com) or from other online or retail vendors.

2. Go to your browser's extension store and search for Web Threat Shield.
 - For Chrome™, go to the [Chrome Web Store](#).
 - For Edge, go to [Microsoft Edge Add-ons](#).
 - For Firefox, go to [Firefox Add-ons](#).
3. Depending on your browser, click either:
 - **Add to Chrome** for Chrome.
 - **Get** for Edge.
 - **Add to Firefox** for Firefox.
4. In the dialog box that opens, click **Add extension**. The **Web Threat Shield Settings** webpage appears.
5. Enter your keycode in the **New keycode** field. For instructions on how to locate your keycode, refer to the [Knowledge Base](#). Then, click **Validate keycode**.
6. In your browser's toolbar, Web Threat Shield appears as an extension and the **Web Threat Shield Features** window opens.



7. Click anywhere on the webpage to close the Features window.
-

Understanding filter results

When you run an internet query such as a Google search, Web Threat Shield displays icons and messages that give you safety information about each website returned as a result of the search.




This topic contains three types of scenarios:

- [What happens when you run an internet search.](#)
- [What happens when you are in a website.](#)
- [What happens when you encounter a block page.](#)


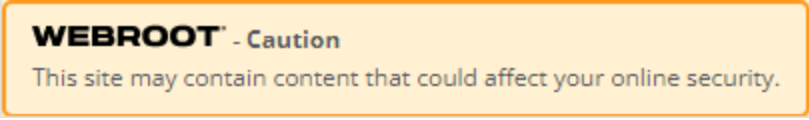
Running an internet search

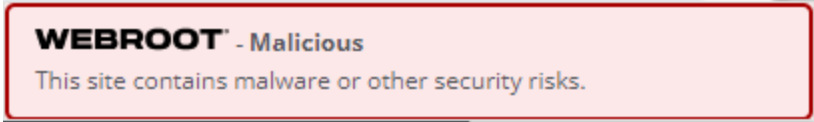
When you run an internet search, you get a list of potential websites that match your search.

Before each website listed in your returned search results is an icon, which indicates 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. |




When you hover over each icon, a message displays with additional information. The following table describes those messages.

| MESSAGE | DESCRIPTION |
|--|---|
|  <p>WEBROOT® - Trustworthy It's safe to go ahead.</p> | <p>Trustworthy. This website is safe to visit.</p> <p>These are known websites with strong security practices, and rarely exhibit characteristics that expose you to security risks. There is a very low probability that you will be exposed to malicious links or payloads.</p> |
|  <p>WEBROOT® - Caution This site may contain content that could affect your online security.</p> | <p>Caution. This website might contain content that could affect your online security.</p> <p>These are generally benign websites, but have exhibited some characteristics that suggest security risk. There is some probability that you will be exposed to malicious links or payloads.</p> |


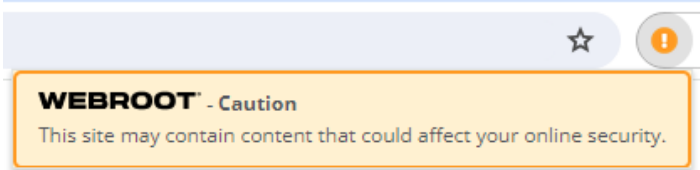
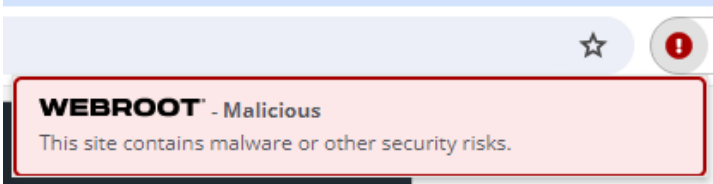
| MESSAGE | DESCRIPTION |
|--|--|
|  <p>WEBROOT™ - Malicious This site contains malware or other security risks.</p> | <p>Malicious. This website contains malware or other security risks.</p> <p>These are high-risk websites. There is a high probability that you will be exposed to malicious links or payloads.</p> |

Visiting a website

When you visit a website, in the browser toolbar, an icon displays indicating the safety level of each website. The following table describes those icons and their meaning.

| ICON | DESCRIPTION |
|---|---|
|  WEBROOT® - Trustworthy It's safe to go ahead. | Trustworthy. This website is safe to visit. |
|  WEBROOT® - Caution This site may contain content that could affect your online security. | Caution. This website might contain content that could affect your online security. |
|  WEBROOT® - Malicious This site contains malware or other security risks. | Malicious. This website contains malware or other security risks. |

If you hover over each icon, a message displays with additional information. The following table describes those messages.

| MESSAGE | DESCRIPTION |
|---|---|
|  <p>The image shows a Webroot notification bar with a green background. On the right side, there is a star icon and a green circle with a white checkmark. The text reads: WEBROOT® - Trustworthy and <i>It's safe to go ahead.</i></p> | <p>Trustworthy. This website is safe to visit.</p> <p>These are well-known websites with strong security practices, and rarely exhibit characteristics that expose you to security risks. There is a very low probability that you will be exposed to malicious links or payloads.</p> |
|  <p>The image shows a Webroot notification bar with a yellow background. On the right side, there is a star icon and a yellow circle with a white exclamation mark. The text reads: WEBROOT® - Caution and <i>This site may contain content that could affect your online security.</i></p> | <p>Caution. This website might contain content that could affect your online security.</p> <p>These are generally benign websites, but have exhibited some characteristics that suggest security risk. There is some probability that you will be exposed to malicious links or payloads.</p> |
|  <p>The image shows a Webroot notification bar with a red background. On the right side, there is a star icon and a red circle with a white exclamation mark. The text reads: WEBROOT® - Malicious and <i>This site contains malware or other security risks.</i></p> | <p>Malicious. This website contains malware or other security risks.</p> <p>These are high-risk websites. There is a high probability that you will be exposed to malicious links or payloads.</p> |

Encountering a block page

Web Threat Shield displays a warning before loading high-risk websites. If you try to proceed to a website that Webroot determines is malicious, a block page displays.

You can do one of three things:

- Click **Go back to safety** to return to your previous webpage.
 - Click **Request Review** to send a request to Webroot's threat researchers to review and verify the site. For more information, see [Requesting a website review](#).
 - Click **Unblock page and continue** (not recommended) to remove the block page and go to the high-risk website. Only unblock websites if you are familiar with them or if you have verified that they are not threatening to your personal information or security.
-

Requesting a website review

When you are browsing the internet, you might encounter a block page. This block page displays because the site you are going to is classified as malicious, according to Webroot.

If you think that the website is incorrectly classified, then you can send a request to Webroot's threat experts to review the website and potentially reclassify it.

To request a website review:

1. On the block page, click **Request Review**. The page expands.
 2. Optionally, enter any additional information, such as more details about the website. You can also enter your email address if you want to allow Webroot to contact you regarding your request.
 3. Click **Submit**. Webroot will examine the reputation of the website and determine whether the website should be reclassified.
-

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.](#)
 - [Look for the answer in our Knowledge Base and FAQs.](#)
 - [Look for the answer in our online documentation.](#)
 - [Enter a help ticket.](#)
 - [Connect to the Webroot Security forum.](#)
-