ADD EXCLUSIONS TO MALWAREBYTES

Malwarebytes for Windows can block items, including websites, applications, and files, that are not inherently malicious. The most common non-malicious items are Potentially Unwanted Programs (PUPs) and Potentially Unwanted Modifications (PUMs). There are some exceptions where Malwarebytes may flag an item as malicious that you trust. To stop Malwarebytes from blocking an item you trust, add the item to your exclusions. When an item is excluded, it is omitted from future scans.

In Malwarebytes, there are four types of exclusions you can add:

- Exclude a Specific File or Folder
- Exclude a Specific Website
- Exclude an Application that Connects to the Internet
- Exclude a Previously Detected Exploit

Malwarebytes exclusions

1. Open Malwarebytes.
2. Click **Settings**, then click the **Exclusions** tab.
3. To add an item to the exclusion list, click **Add Exclusion**.
4. Select the type of exclusion you want to add.
5. Click **Next**, then follow the next prompt to add your exclusion and confirm your changes.

Exclude a File or Folder

Excluding a file or folder instructs Malwarebytes to ignore the file's location. If you exclude a folder, every file and folder inside is also excluded.

1. Click **Exclude a File or Folder**, then click **Next**.
2. Click **Select Files** or **Select Folder**.
3. Choose the file or folder you wish to exclude, then click **Open**.
4. Under **How to Exclude**, choose how you would like to exclude the file or folder.

Exclude a Website

1. Add a website or IP address to your exclusions. When you are adding a website, add the website with and without the world wide web (www.) prefix.
2. Click **Exclude a Website**, then click **Next**.
3. Click **Exclude a domain** or **Exclude an IP Address**.
4. Enter the URL or IP Address.
5. Click **OK** to confirm your changes.

Exclude an Application that Connects to the Internet

To prevent Malwarebytes from blocking an application you trust, exclude the application executable.

1. Click **Exclude an Application that Connects to the Internet**, then click **Next**.
2. To find and exclude the application, click **Browse...**.
3. Choose the application executable you wish to exclude, then click **Open**.
4. Click **OK** to confirm your changes.

Exclude a Previously Detected Exploit

When you are excluding an exploit, Malwarebytes uses a code called an MD5 hash. An MD5 hash is unique and helps Malwarebytes identify the specific application that Exploit Protection blocked.

1. Click **Exclude a Previously Detected Exploit**, then click **Next**.
2. Click **Select...**.
3. Select an exploit to ignore, then click **OK**.
4. Under **Application**, enter the name of the application you are excluding.
5. Click **OK** to confirm your changes.

Once an exclusion is added to Malwarebytes, the exclusion begins to take effect immediately.