

Remove Mac Defender (Uninstall Guide)

This is a self-help guide. Use at your own risk.

What this infection does:

Mac Defender is a fake rogue anti-spyware program that for the Mac OS operating system. This infection is spread through the use of advertisements on web sites that pretend to be fake online scanners. When these fake scans are finished, it will state that your computer is infected and then automatically download the Mac Defender program onto your computer. Once the program has finished downloading, the installer will start and prompt you to install the program.

Once the program is installed it will be configured to start up automatically when you login to your Mac. Once running it will pretend to scan your computer and then state that there are numerous files on your computer that are infected. If you attempt to clean these fake infections, though, the program will state that you must first purchase a license before it will allow you to do so. After the scan the Control Center screen for Mac Defender will be updated to state that your computer is infected and at Risk. Regardless of the information presented by this program, you should not purchase this program as all of this information is false.

Unfortunately, when Mac Defender is installed on your computer it will also be added to your accounts Login Items so that the program is launched every time you login to your Mac. As there is no Dock icon for this application, it is also not easily closed and will instead require you to terminate its process through the Activity Monitor before you are able to remove the application from your computer.



While the program is running it will also display fake security alerts that are further used to scare you into thinking that your computer has a serious problem. Some of these alerts include:

The system is infected

Your system is infected. It's highly recommended to cleanup your system to protect critical information like credit card numbers, etc.

Unregistered Copy

Sorry, the copy of your program is unregistered. Register to have an ability to cleanup your system.

Virus Found

Infected file detected:

Virus: Dialer

File: Safari

Virus Found

Infected file detected:

Virus: Worm

File: clri

Virus Found

Infected file detected:

Virus: Worm

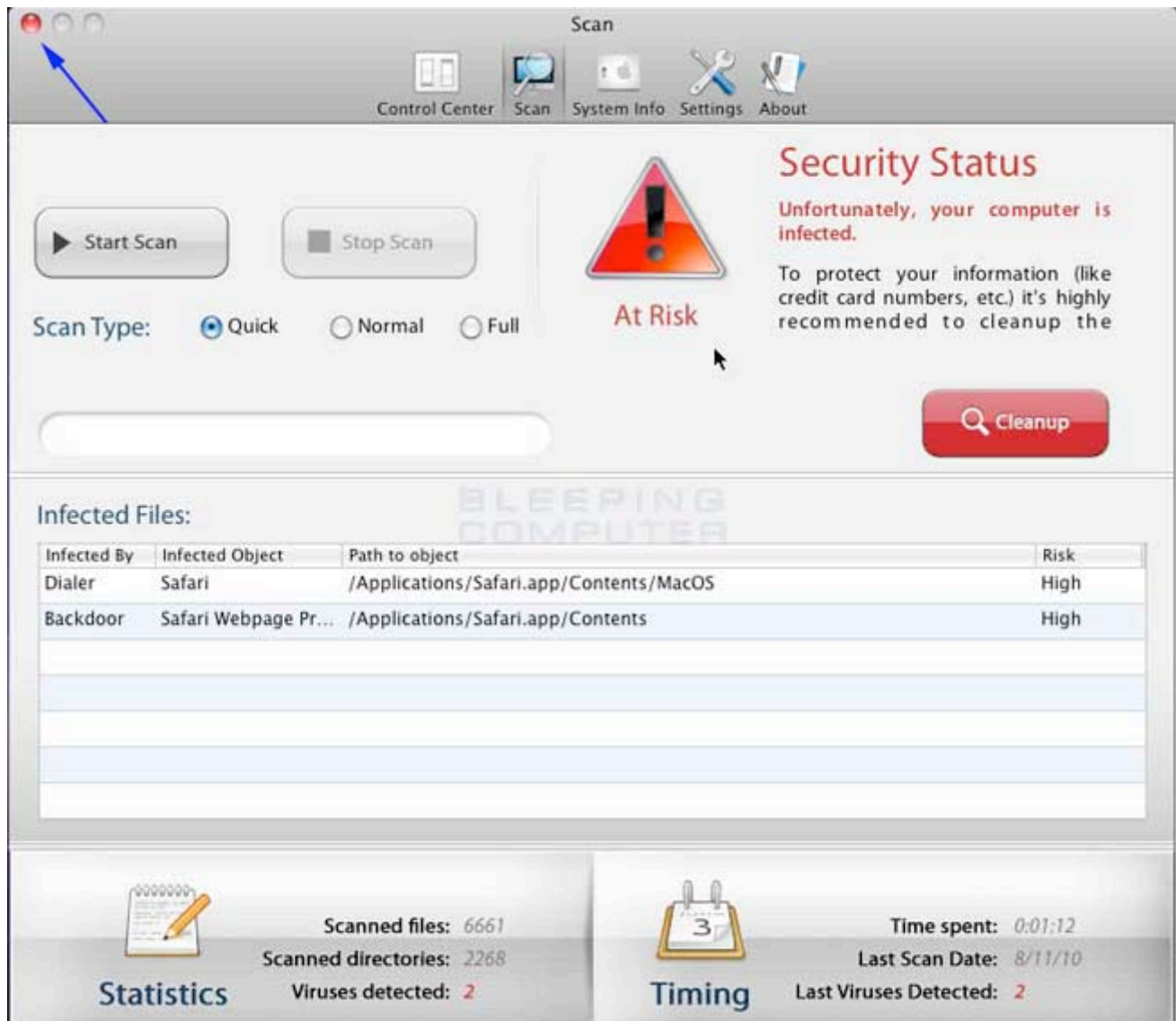
File: Software Update

Just like the fake scan results, these alerts are also fake and are only being used to scare you into purchasing the program. Therefore, please ignore them and do not purchase the program. Last, but not least, while the program is running it will also open up web sites to various pornographic sites.

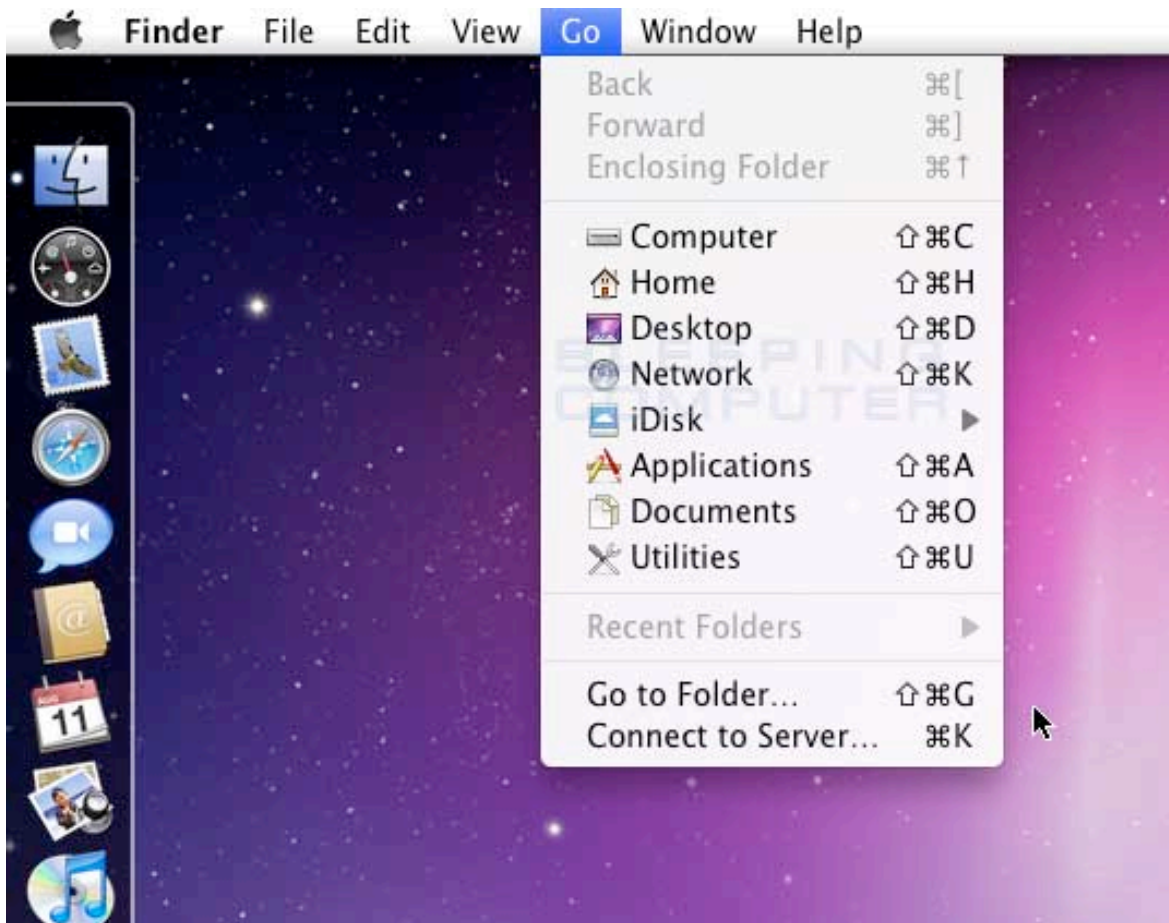
As you can see, Mac Defender was created to scare you into thinking your computer has a severe security problem so that you will then purchase this program. For no reason should you purchase Mac Defender , and if you already have, you should contact your credit card company and dispute the charges stating that the program is a computer infection. Finally, to remove this infection, and any related malware, please use the removal guide below.

Manual Removal Instructions for Mac Defender:

1. Print out these instructions so it will be easier to reference it as you follow these steps.
2. As **Mac Defender** will stay on top of any other programs that are running, we first want to close the program so that we can see the other screens that we need to open during this cleaning process. Please close this window by clicking on the red close (X) button in the top left of the **Mac Defender** Windows. The button that you need to click in order to close the window is shown below:



3. Next you should click on empty portion of your desktop so that the **Finder** is selected. Once it is selected, click on the **Go** button and select **Utilities** as shown in the image below.



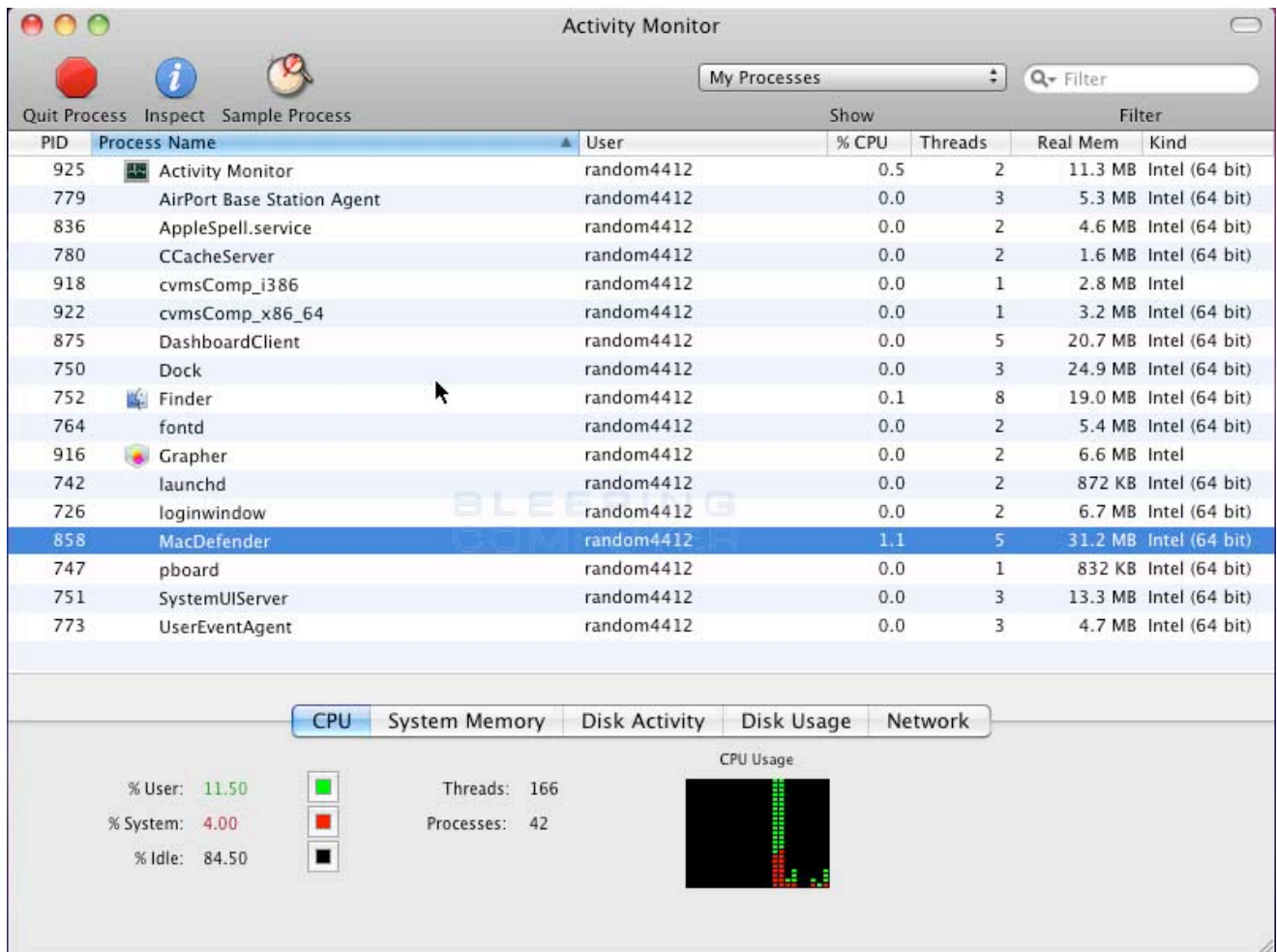
4. The **Utilities** folder should now appear as shown in the image below.



1.

Locate the **Activity Monitor** icon and double-click on it.

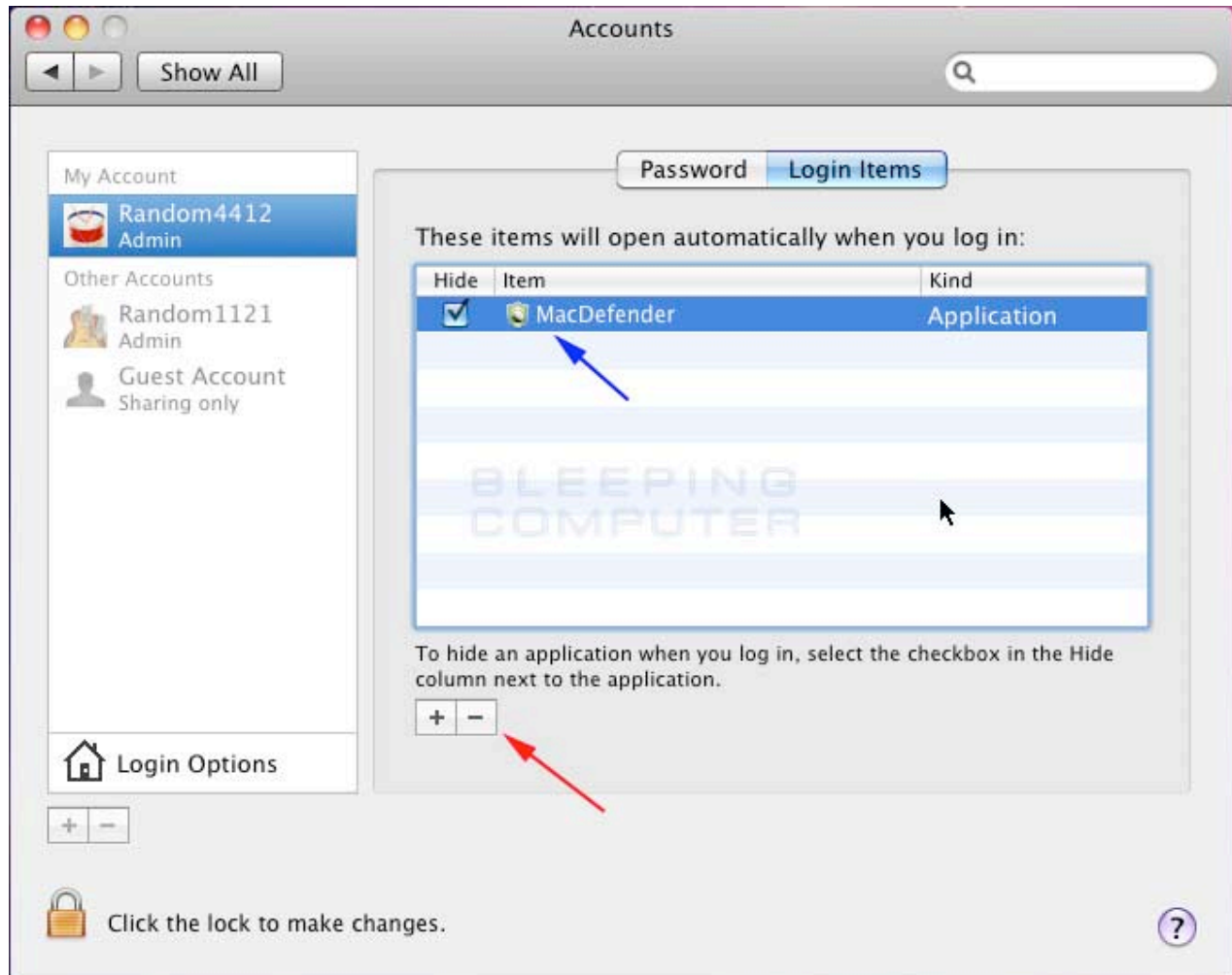
5. The Activity Monitor should now be displayed on your screen. This program lists all the processes that are currently running on your Mac OS and allows us to terminate specific programs that may be running. Scroll through the list of processes and left click on the process named **MacDefender** as shown in the image below.



Once the process is selected click on the **Quit Process** button. When a prompt appears asking if you are sure you want to quit the **MacDefender** process, please click on the **Force Quit** button. When you have finished, **Mac Defender** should no longer be running on your Mac and you can now close the **Activity Monitor** and the **Utilities** window.

6. While still at the Finder, click on the **Go** button and select the **Applications** menu option. When the Applications folder is displayed, scroll through the list of programs until you see a program named **MacDefender**. When you find the program, right-click on it and select the **Move to Trash** menu option. If MacOS prompts you for your password, please enter it. The MacDefender application will now be removed from the operating system.

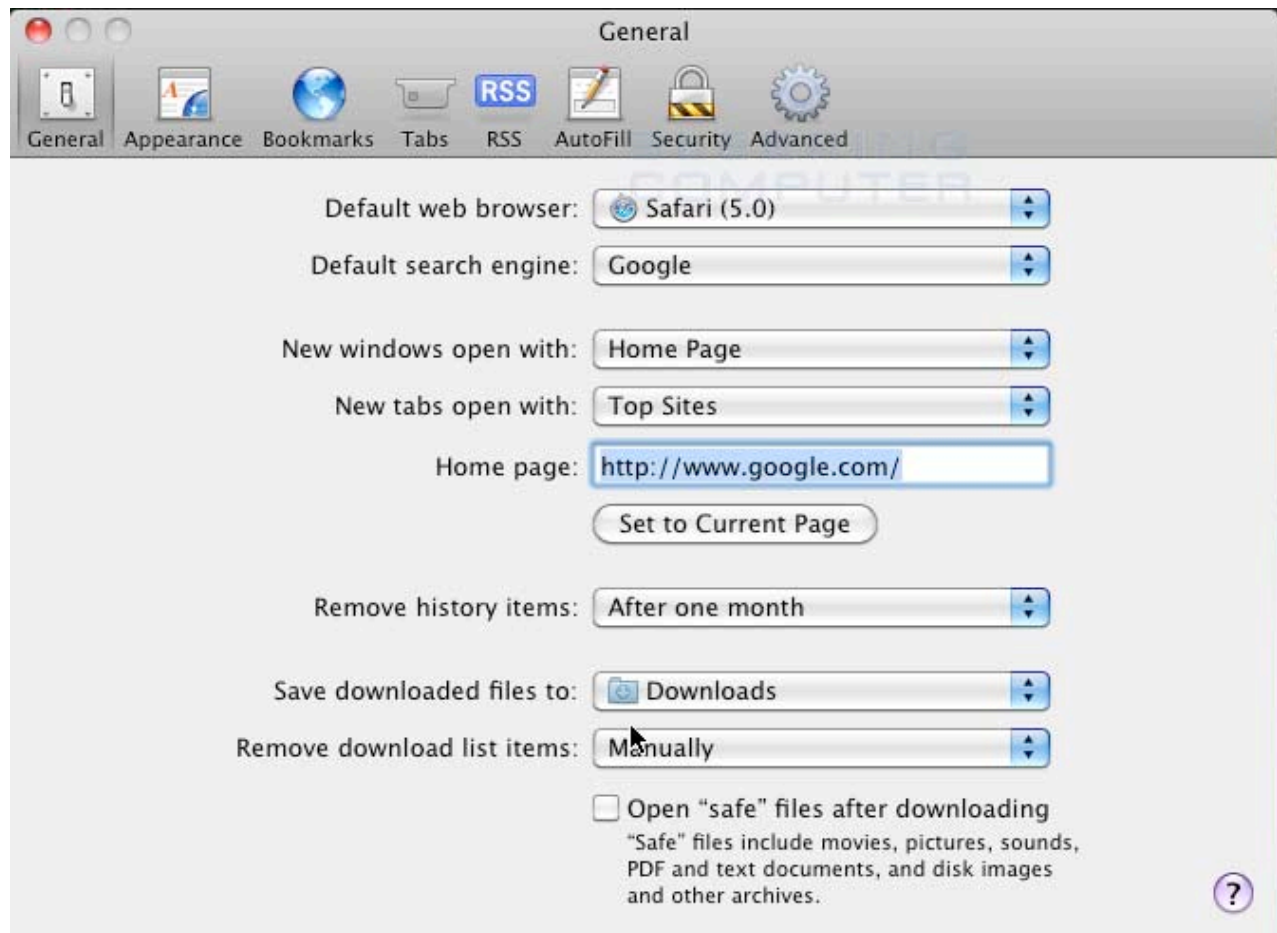
7. Now click on the **Apple Menu** () and select the **System Preferences** menu option. When the System Preferences screen opens, select the **Accounts** option under the System category. When the Accounts screen opens, click on the **Login Items** button. This will open a screen, similar to the one below, that displays a list of programs that will automatically start for this particular user when they login to the operating system.



Look through the list of programs that are starting automatically, and single click on the entry named **MacDefender**. Once it is selected, click on the **minus (-) sign** button, as indicated by the red arrow in the image above. Once you click on the minus button the Mac Defender entry will be removed and MacOS will no longer attempt to start it when you login.

8. Now that **Mac Defender** is no longer running, we need to change a setting in Safari so that these types of programs are not automatically run on your **computer** in the future. By default Safari opens and launches programs that it considers safe to run. These programs include movies, pictures, sounds, PDFs, text documents, archives, and disk images. Due to this, these types of infections are able to be downloaded and automatically run on your Mac. To fix this, start the **Safari** program and then click on the **Safari** menu option. From the Safari drop down menu,

select **Preferences**. This will open the Preferences screen as shown below. When the screen opens, if you are not on the General settings screen, please click on the **General** button.



You should now uncheck the checkbox labeled **Open "safe" files after downloading** as shown in the image above. After unchecking this box you can close the Preferences screen and Safari.

Your computer should now be free of the **MacDefender** program and Safari should be secure so that it does not automatically launch these types of programs.

Associated Mac Defender Files:

```
/Applications/MacDefender.app/  
/Applications/MacDefender.app/Contents  
/Applications/MacDefender.app/Contents/Info.plist  
/Applications/MacDefender.app/Contents/MacOS  
/Applications/MacDefender.app/Contents/MacOS/MacDefender  
/Applications/MacDefender.app/Contents/PkgInfo  
/Applications/MacDefender.app/Contents/Resources  
/Applications/MacDefender.app/Contents/Resources/About-Back.png  
/Applications/MacDefender.app/Contents/Resources/AboutD.nib
```

/Applications/MacDefender.app/Contents/Resources/AboutMBMI.png
/Applications/MacDefender.app/Contents/Resources/affid.txt
/Applications/MacDefender.app/Contents/Resources/ControlCenterD.nib
/Applications/MacDefender.app/Contents/Resources/Curing_1.png
/Applications/MacDefender.app/Contents/Resources/Curing_2.png
/Applications/MacDefender.app/Contents/Resources/Curing_3.png
/Applications/MacDefender.app/Contents/Resources/Curing_4.png
/Applications/MacDefender.app/Contents/Resources/Curing_5.png
/Applications/MacDefender.app/Contents/Resources/Curing_6.png
/Applications/MacDefender.app/Contents/Resources/Curing_7.png
... <numerous other image and media files>