

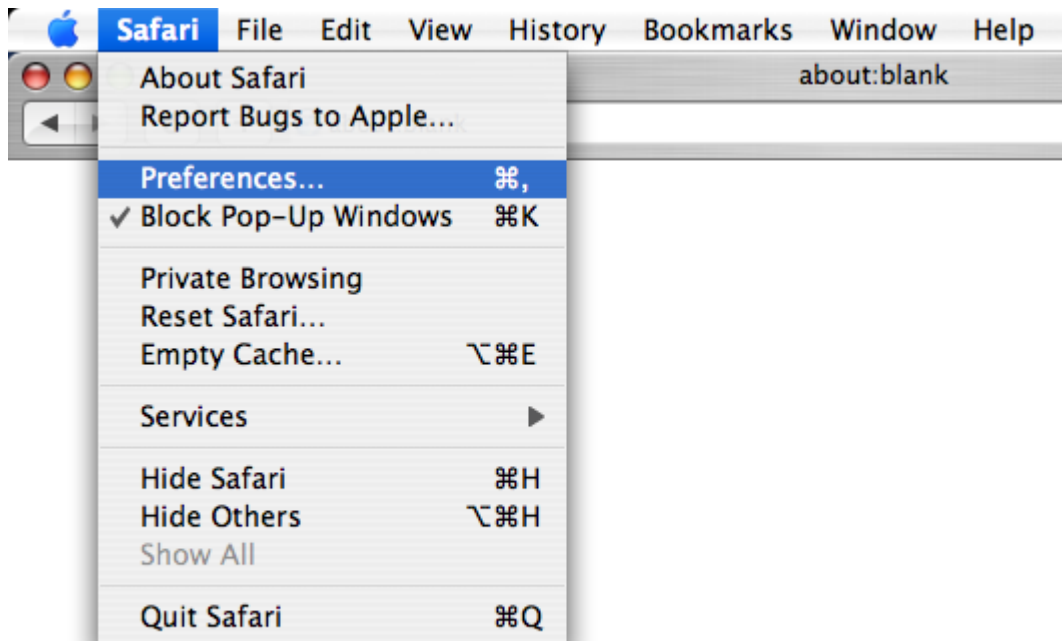


How to Secure the Apple Macintosh Safari Web Browser

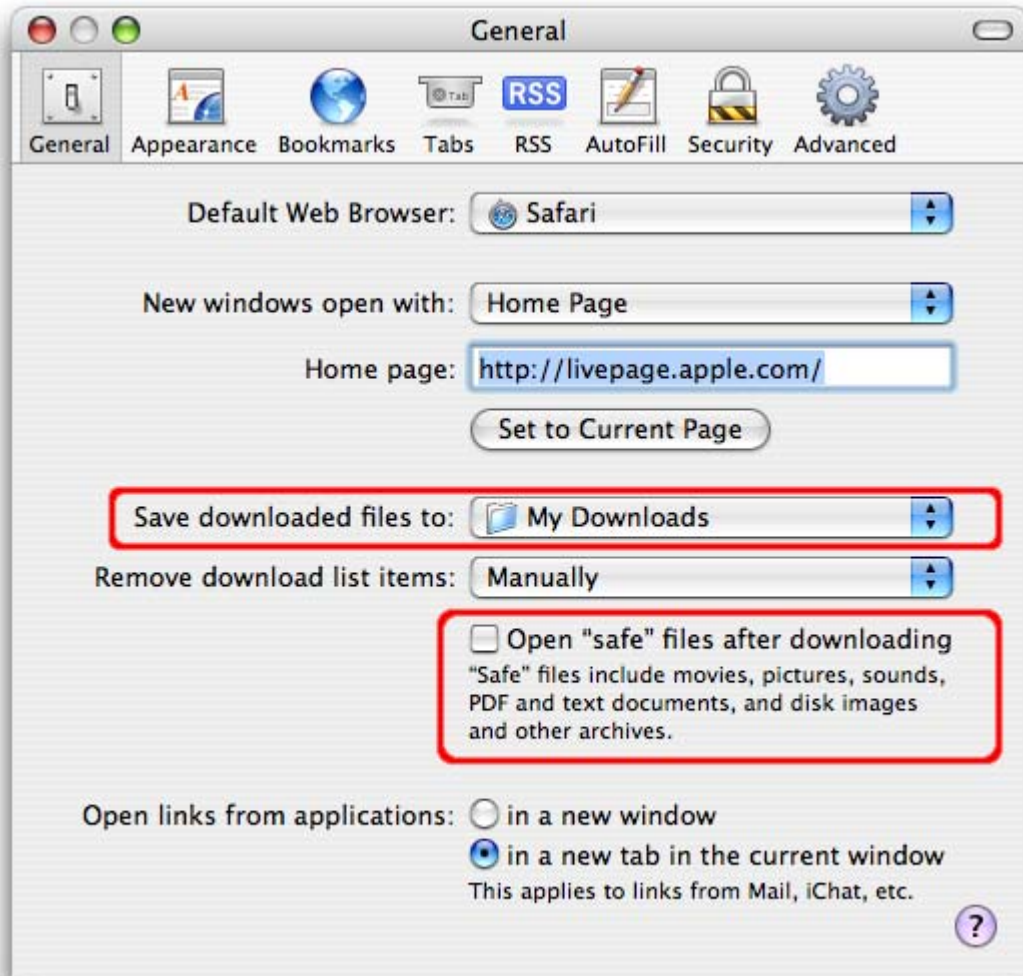
This section describes steps to disable various features in Safari. Note that some menu options may change over time, and you should adapt the steps below as appropriate.

In order to change settings, select **Safari** and then select **Preferences...**

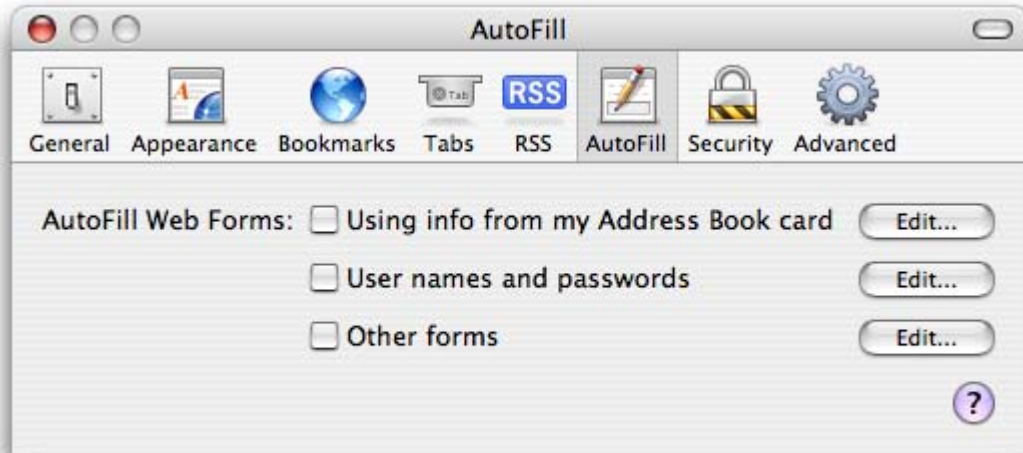
Note that on the Safari menu, you can also select the option "Block Pop-up Windows". This option will prevent sites from opening another window through the use of scripting, or active content. Be aware that while pop-up windows are often associated with advertisements, some sites may attempt to display content relevant to your usage of the site in a new window. Therefore, setting this option may disable the functionality of some sites.



Once you select the **Preferences** menu, the window depicted below will open. The first tab to examine is the **General** tab. On this tab, you can set up many options such as **Save downloaded files to:** and **Open "safe" files after downloading.** We recommend that you save downloaded files to a temporary folder that you create for downloading files. We also recommend that you deselect the **Open "safe" files after downloading** option.



The next section of interest is the **AutoFill** tab. On this tab, you can select what types of forms your browser will fill in automatically. In general, we recommend against using AutoFill features. If someone can gain access to your computer, or to the data files, then the AutoFill feature may permit them even easier access to other sites that they would not otherwise have the ability to access. However, if used with appropriate protective measures, it may be acceptable to enable AutoFill. We recommend using filesystem encryption software such as OS X FileVault to provide additional security for files that reside in a user's home directory.



The **Security** tab provides several options. The **Web Content** section permits you to enable or disable various forms of scripting and active content. We recommend disabling the first three options in this section, and only enabling them when you require the functionality of these features. We recommend selecting the **Block Pop-up Windows** option. Remember that this option will prevent sites from opening another window through the use of scripting, or active content. Again, be aware that while pop-up windows are often associated with advertisements, some sites may attempt to display content relevant to your usage of the site in a new window. Therefore, setting this option may disable the functionality of some sites.

It is safer to use Safari without plug-ins and Java, so we recommend disabling the options **Enable plug-ins** and **Enable Java**. It is also safer to disable JavaScript. However, many web sites require JavaScript for proper operation.

In this dialog you can disable cookies and can also view or remove cookies that have been set. In general, we recommend disabling cookies and enabling them only when you visit a site that requires their use. At this point, you should determine if the site is trustworthy (i.e., contains no malicious content and is securely designed) and determine whether you want to allow cookies to access the site's content. After you are finished visiting the site, we recommend disabling cookies until you need to access a site that requires cookies. You can limit cookies to the sites that you navigate to by selecting the option **Only from sites you navigate to**. This will permit sites that you visit to set cookies, but not third-party sites. Finally, we recommend selecting the **Ask before sending a non-secure form to a secure website** option. This will alert you when data is sent to a secure web site over an insecure channel.

