



# Computer Security

There are some simple steps that everyone should take to help ensure their identity remains safe when working on computers.

- Memorize all of your passwords. Unless you completely know it to be trustworthy, it is better to not allow a website to 'remember' and save your log in information. It is always safer to be sure the settings force you to log in every time you visit.
- Watch for fake emails that may try to "phish" you for information. You may receive an email that appears to be from a website that you use, such as EBay, Amazon or a credit card company. But be aware, these may be phony emails that will take you to a duplicate site. Once you've input your personal information, the criminal who created the mirror site will have it and be able to use it. This is why you should always log in directly at the home page of any website you visit.
- Never input your log on information after clicking on a link to any website.
- When you receive an email that asks you to click on a link and then log on, alert the company that supposedly sent it. They may be able to help put a stop to the problem.
- Unless you know for sure it is legitimate reason from a legitimate site, do not fill out forms or surveys that request personal information. Many of these sites are designed to collect your private data. At best it might be used to spam your mailbox, at worst it could be used to steal your identity.
- Only make online purchases with websites that you know offer secure checkout procedures. If you are not certain, do not give out your credit card details. It is better to be safe and buy from a reputable site where your information will remain secure and private.

*For more information about college campus safety, please visit the national crime prevention council web site at: <http://www.ncpc.org/training/campus-crime-prevention>.*

Below are some valuable ways to manage your personal information online, as well as tips for following safe browsing procedures.

## **Find a Safe Computer**

Please take a moment to think about whether your computer is safe. This is particularly important if the person abusing you may have access to your computer.

## **Edit Privacy Settings on Facebook**

Review steps you can take to manage your personal information on Facebook.

## **Edit Privacy Settings on Twitter**

Review steps you can take to manage your personal information on Twitter.

## Clear History/Cache on Mobile Devices

Quick steps to clear your browsing history on iPhone and Blackberry mobile devices.

## Clear History/Cache on Firefox for PC

Quick steps to clear your browsing history on Firefox (for PC).

## Clear History/Cache on Firefox for Mac

Quick steps to clear your browsing history on Firefox (for Mac).

## Clear History/Cache on Internet Explorer

Quick steps to clear your browsing history on Internet Explorer.

## Clear History/Cache on Safari

Quick steps to clear your browsing history on Safari.

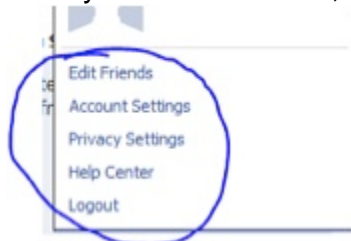
---

## How to Edit Privacy Settings on Facebook

Log in to your Facebook account. Browse to the right and click the **Account** tab.



Once you click **Account**, the following selections will appear:



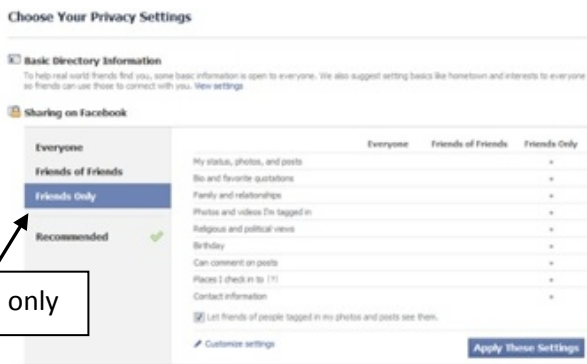
Edit Friends  
**Account Settings**  
Privacy Settings  
Help Center  
Logout

Click on **Account Settings**

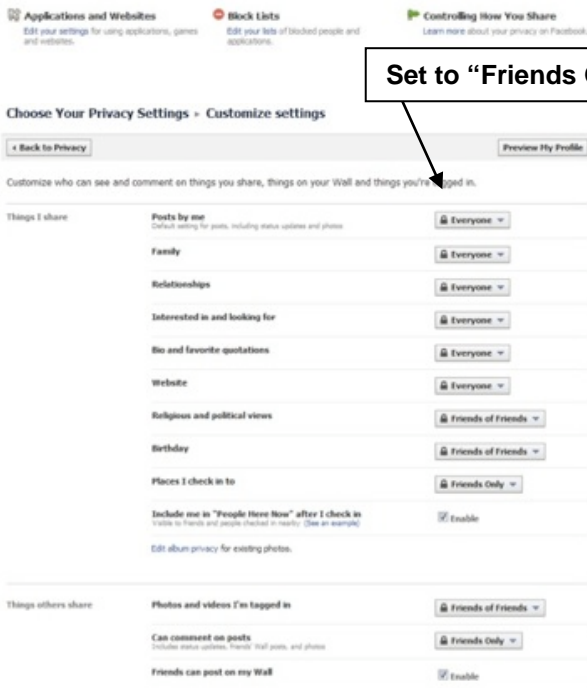
From here you can modify any of your account settings. For example, you can go to Password and click Change. You can then create a more secure password for your account. You can also select a Security Question that makes it more difficult for someone to change your account log in. Scroll to **Privacy** and click **Manage**. (See the windows below for details.)



Name	<a href="#">change</a>
Username	<a href="#">change</a>
Email	<a href="#">change</a>
Password	<a href="#">change</a>
Linked Accounts	<a href="#">change</a>
Security Question	<a href="#">change</a>
Privacy	<a href="#">manage</a>
Account Security	<a href="#">change</a>
Deactivate Account	<a href="#">deactivate</a>

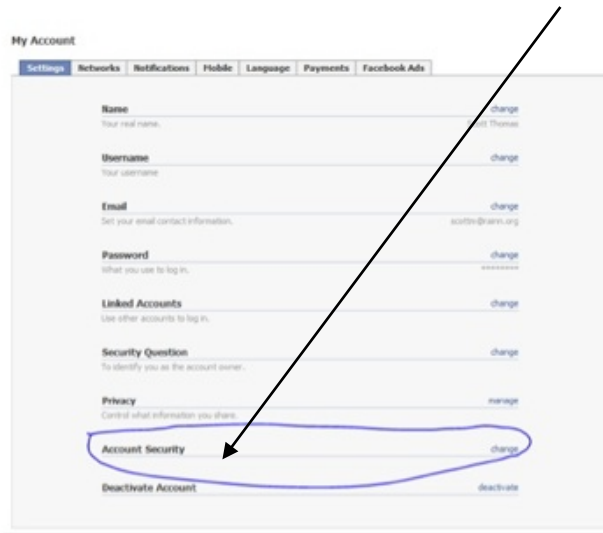


It is recommended that your settings do not allow account access to everyone. Try to maintain it to friends only, as indicated above. Once you have modified your privacy settings to your liking, click **Apply These Settings**. If you want to choose specific information that is viewable or blocked, you can click **Customize Settings**. The screenshot is indicated below.



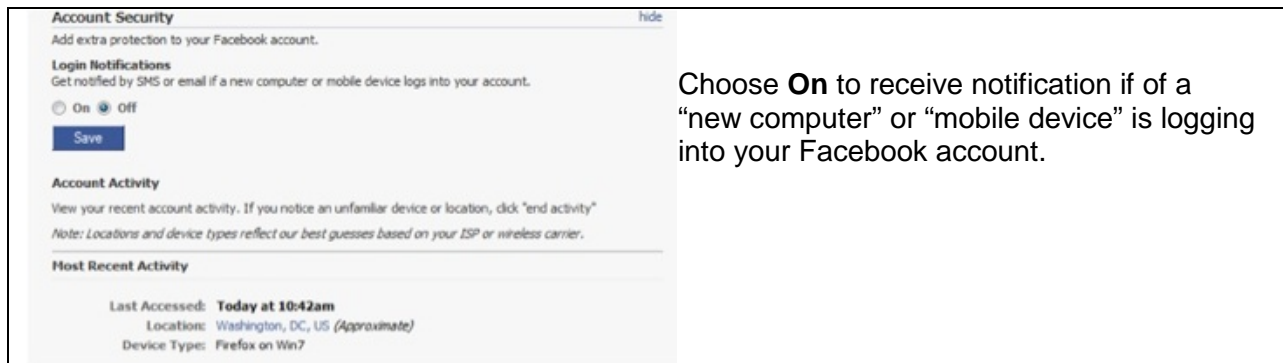
Ideally, you should set these to be visible to **Friends Only** for privacy purposes. Once you have set your preferences, you can return to any page.

Return to **My Account** page and click **Account Security**.



Click **Change** and you can be notified of any account activity.

Your Facebook page and account are now secured to the preferences that you have selected, and will offer you a greater level of privacy, if you have chosen to do so. Remember, it is always recommended that you limit the people that can access your information on ANY type of social networking site. Allowing access to only trusted friends and creating strong account security is a good first step.



Choose **On** to receive notification if of a “new computer” or “mobile device” is logging into your Facebook account.

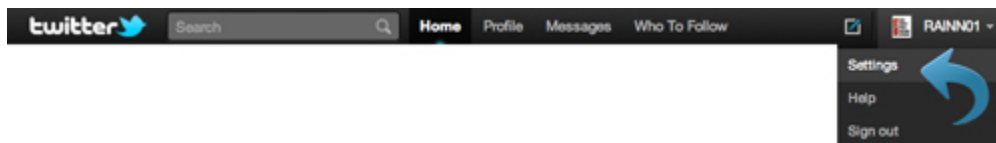
## How to Edit Privacy Settings on Twitter

Sign into your account by going to [Twitter.com](https://twitter.com), browsing to the right and clicking the **Sign In** tab.



Input your login info.

Once you login, click on your Twitter screen name to reveal a drop down menu and the following will appear:



Click on **Settings**.

From here you can edit and modify a number of account settings. Scroll down and you will find areas you can edit privacy settings such as **Tweet Location**, **Tweet Privacy**, and **HTTPS ONLY**.

<p>The screenshot shows the Twitter account settings page with the following sections:</p> <ul style="list-style-type: none"> <li><b>Tweet Location:</b> Includes an option to "Add a location to your Tweets" with a checkbox. Below it, there is explanatory text about how location information is stored and used, and a "Save" button.</li> <li><b>Tweet Media:</b> Includes options to "Display media from people I don't follow" and "Display media that may contain sensitive content", both with checkboxes. There is also an option to "Mark my media as containing sensitive content" with a checkbox and explanatory text.</li> <li><b>Tweet Privacy:</b> Includes an option to "Protect my Tweets" with a checkbox. Below it, there is explanatory text about how protected tweets are visible.</li> <li><b>HTTPS Only:</b> Includes an option to "Always use HTTPS" with a checkbox. Below it, there is explanatory text about using a secure connection.</li> </ul> <p>At the bottom of the settings page, there is a "Save" button and a "Deactivate my account" link.</p>	<ul style="list-style-type: none"> <li>• <b>Adding a location</b> to your Tweets can leave you exposed to predators. If you choose to check this box, please make sure you are aware of who is following you and feel comfortable with them knowing where you are.</li> <li>• When you <b>protect your Tweets</b> you are prohibiting them from being seen by the public. This is a good option if you only want to tweet to a specified group of people. NOTE: Tweets posted prior to protecting your Tweets may still be publicly visible in some places.</li> <li>• Selecting <b>HTTPS ONLY</b> will help protect your account information by using a secure connection where possible to keep things encrypted.</li> </ul>
--	--

## Blocking a user on Twitter

Blocking a user on Twitter will prevent them from following you and mentioning/replying to you in Tweets. Twitter does not notify a user when you block them. Please be aware that if you don't protect your Tweets, they will still be visible to the users you block.

### To block a user:

- Go to the profile page of the person you wish to block.
- Click the person icon (see below).
- Select Block Spammer from the options listed in the drop-down menu.



Remember, it is always recommended that you not only limit the people that can access your information on ANY type of social networking site, but that you limit the information you provide.

Choosing options like protecting your tweets or hiding your location are good practices, but even better is to share no unnecessary personal information on social networking sites that you would be uncomfortable being seen publicly. Limiting the personal information you share is the best way to maintain your privacy online and stay out of potentially dangerous situations.

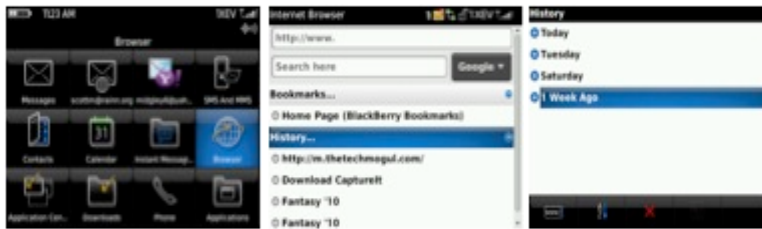
## How to Clear History / Cache on Mobile Devices

### iPhone



Select **Settings**, then **Safari**.  
Choose **Clear History**, then confirm **Clear History**.

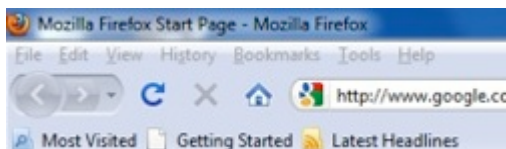
### Blackberry



Press **Browser** then select **History**.  
Choose what time frame you wish to delete and click the **red X**.  
Your browsing history is now deleted.

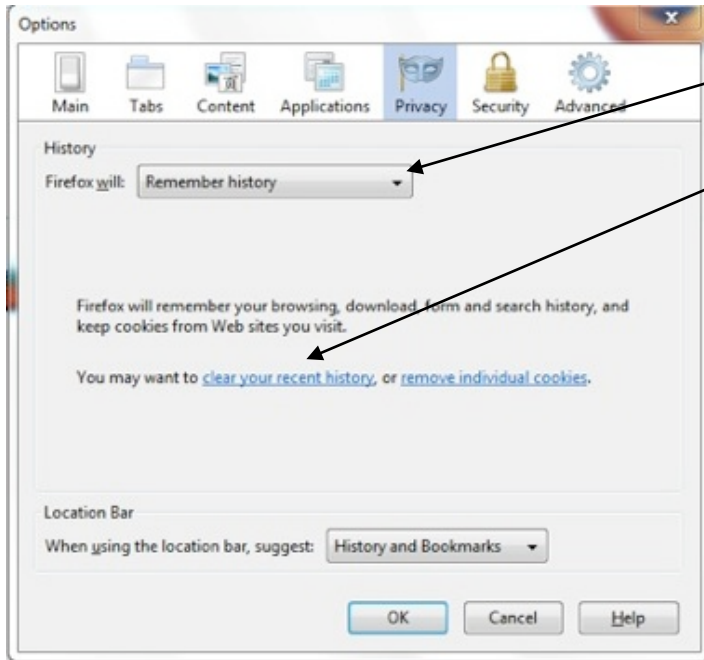
## How to Clear History / Cache on Firefox (PC)

From an open Firefox browser, click **Tools**.



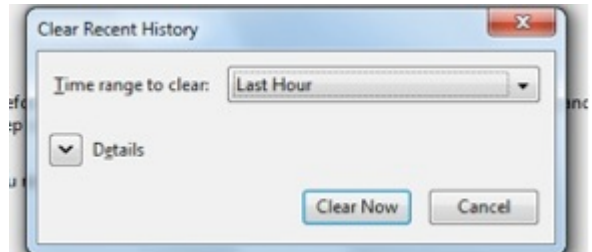
Click **Options** and the following box pops up.



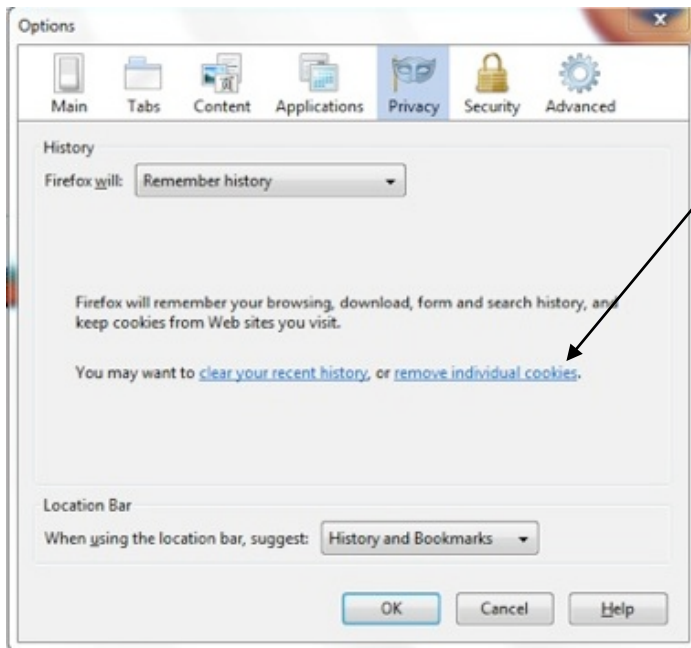


Keep the "Firefox will:" dropdown box on Remember history for this process:

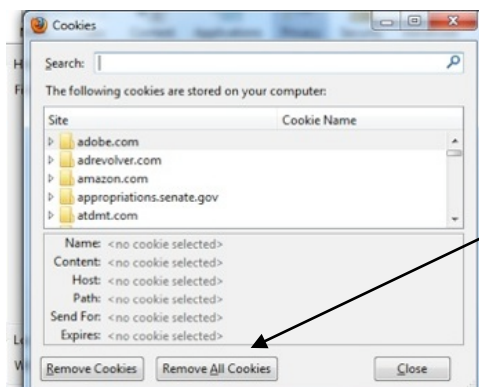
From there, click the [clear your recent history](#) link. The box below will appear:



Once you have selected which **Time range to clear**, click **Clear Now**



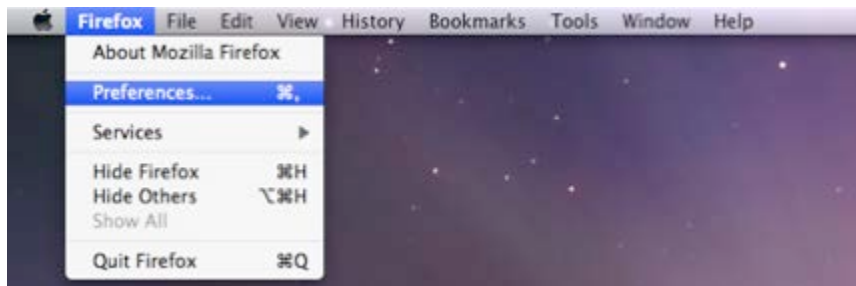
Now, click the link for **Remove Individual Cookies**.



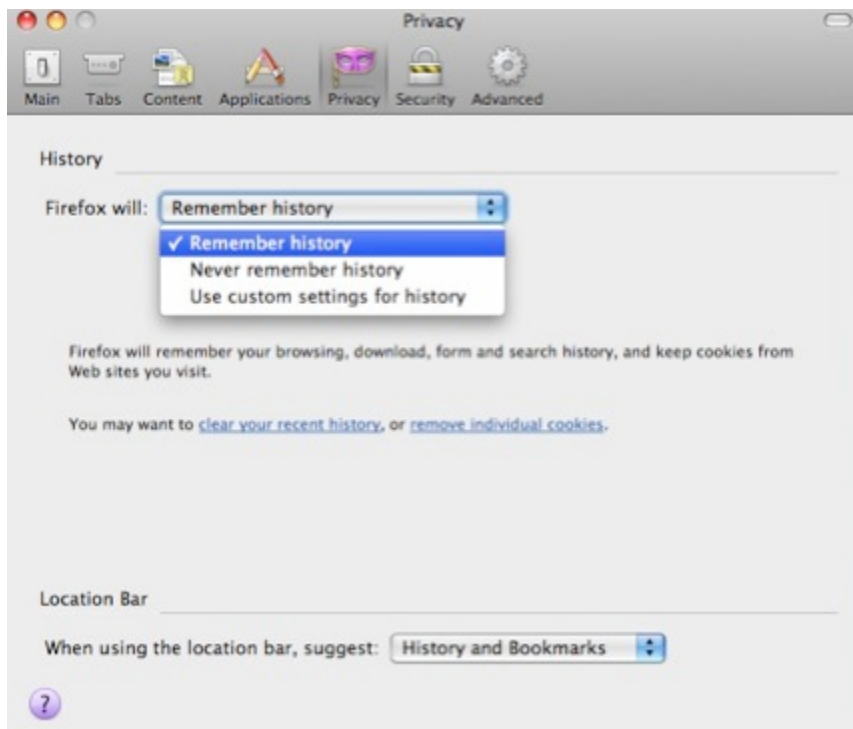
Click **Remove All Cookies** to clear all of the cookies within your browser.

## How to Clear History / Cache on Firefox (Mac)

Click on **Firefox** on the top and select **Preferences**.



Select the **Privacy** tab, and the following appears:



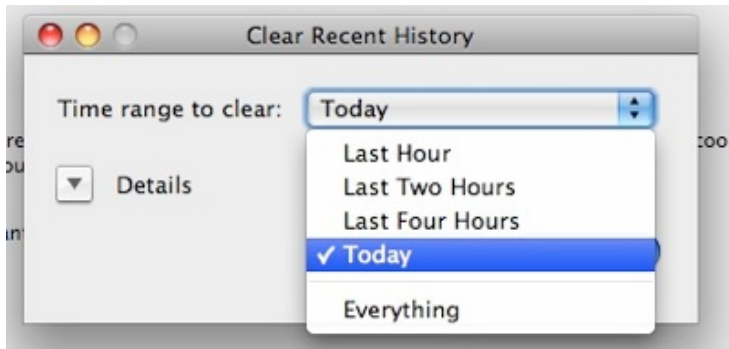
Choose the setting to manage your browsing history.

From here, you can also clear your recent history or remove individual cookies for further security.

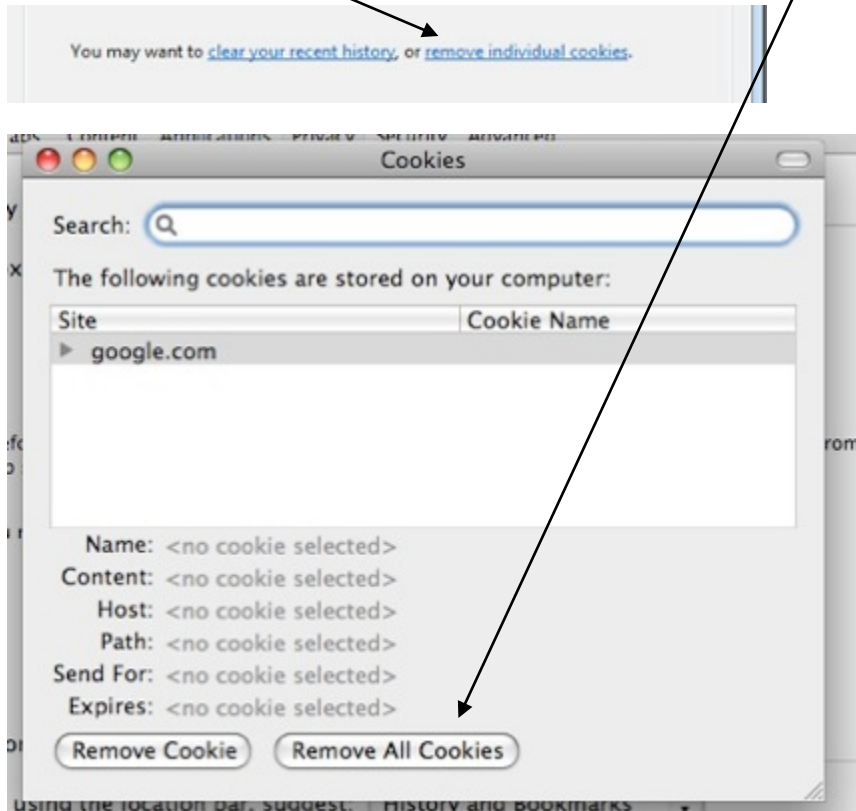
The following screen-shots will walk you through this process.

Click **Clear Recent History** and select the time range to clear.





Click **Remove individual cookies** and select **Remove All Cookies**.



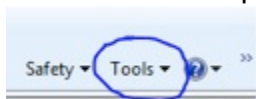
Select either **Remove Cookie** to remove individual cookies or **Remove All Cookies** to clear all of your cookies.

To turn off **Remember Passwords for Sites**, simply click the check box next to it. If you want to keep it on, but set up exceptions for sites that you want to retain saved passwords for, then you can set that up through the **Exceptions** button on the right.

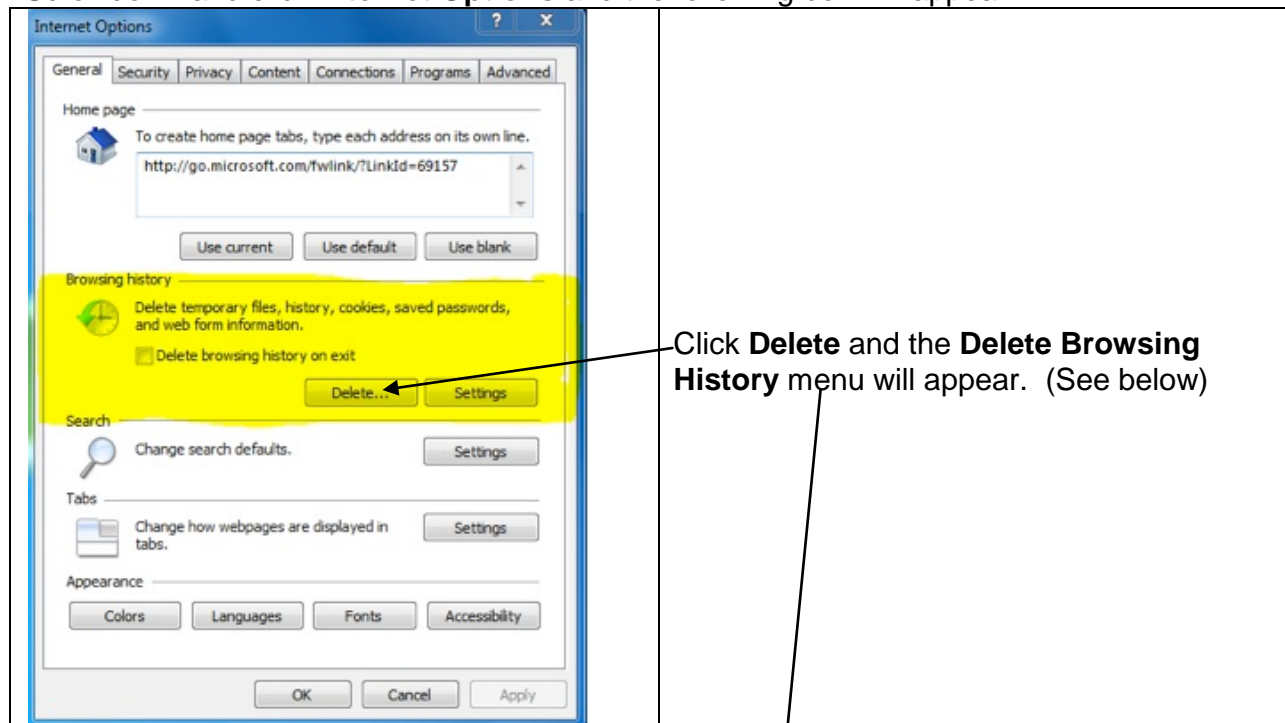


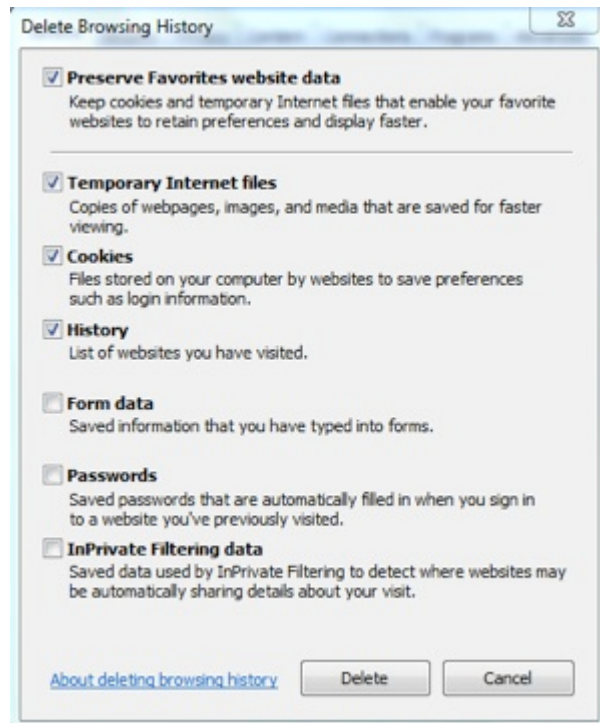
## How to Clear History / Cache on Internet Explorer

On an Internet Explorer 7 browser page, click on **Tools**.



Scroll down and click **Internet Options** and the following box will appear:



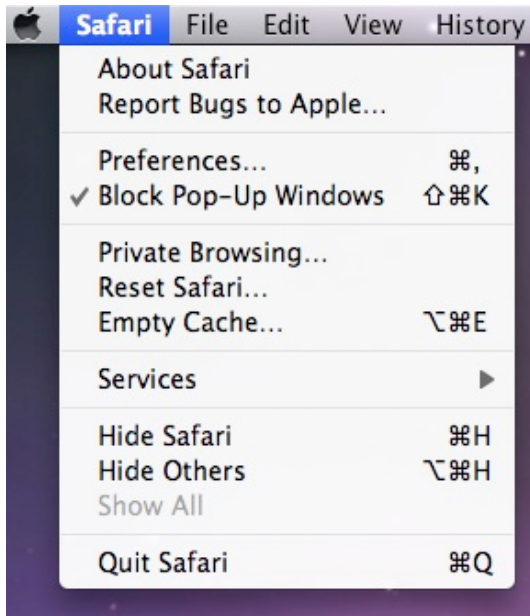


You can also set a specific time frame that you would like Internet Explorer 7 to save or delete browsing history.

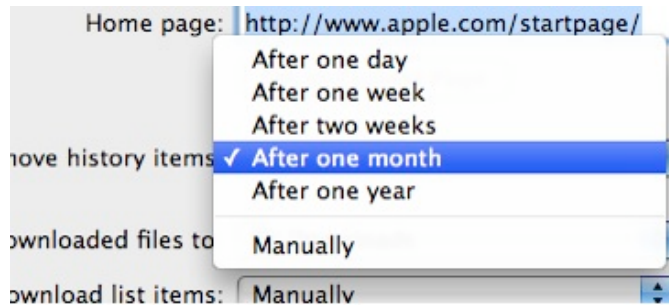


## How to Clear History / Cache on Safari

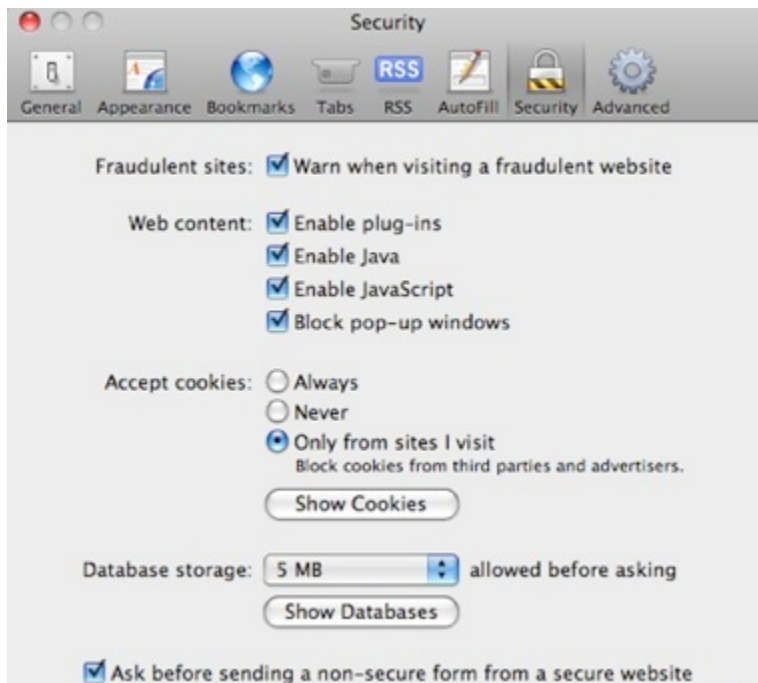
1. Click **Safari** and scroll to **Preferences**.



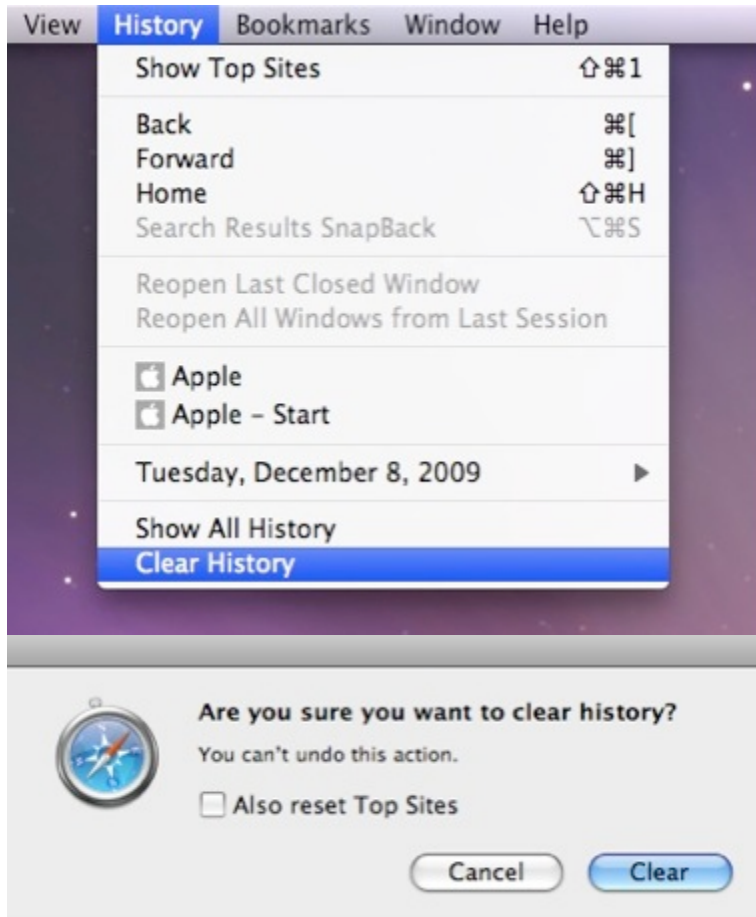
2. On the **General** tab.



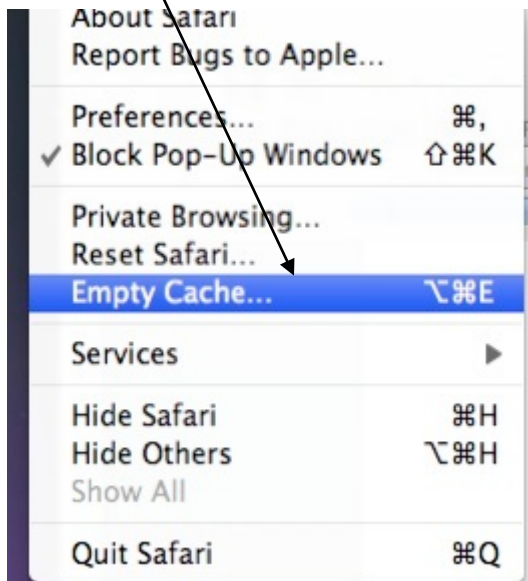
3. Click the **Security** tab and choose whether to block or allow cookies.



Once all settings have been set, go to **History** and scroll to **Clear History**.



To clear the cache, go to **Safari** and scroll to **Empty Cache**.



Then,



Click the **Empty** button and you are now ready to go.