Unit - IX

How to secure Web browsers

By completing module you will be able to understand and learn the following.

What is Web Browser?

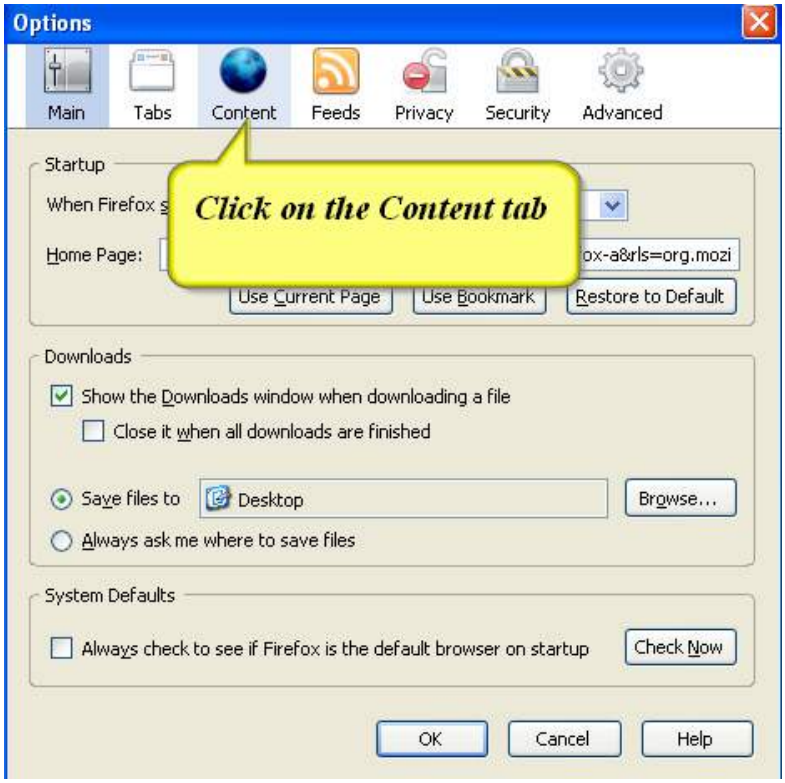
- **How to securing the Micro soft Internet Explorer**
- **How to securing the Firefox web browser**

Mozilla Firefox

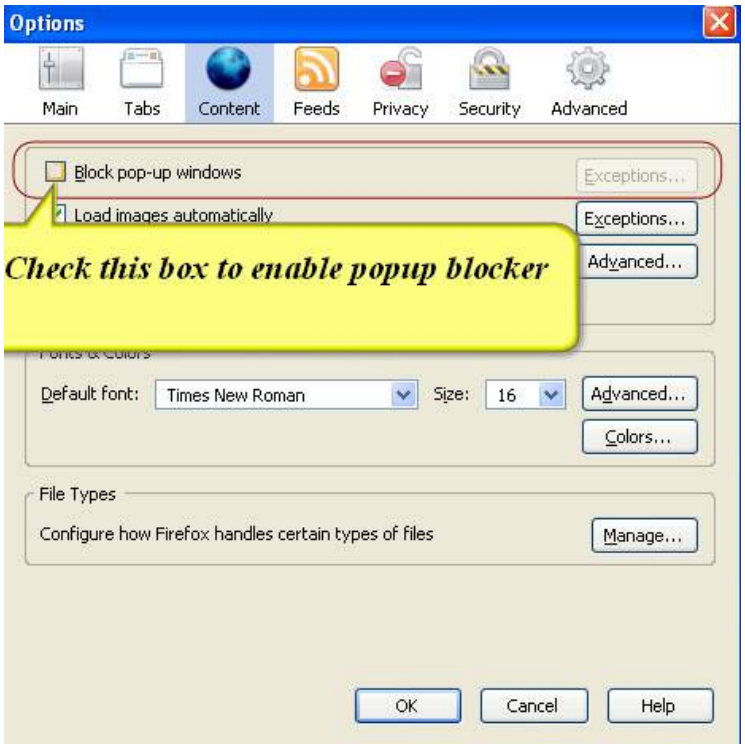
This is the second most popular web browser that people use to access the Internet and consequently needs coverage as well. The following instructions are for Mozilla Firefox running on a Microsoft Windows machine. The most popular version 1.5 and 2.0 all offers

Pop-up Blockers:

As with IE, Mozilla Firefox, henceforth Firefox, also provides a Pop-up blocker.
1.click '**Tools|Options**' menu and then click '**Content**' tab

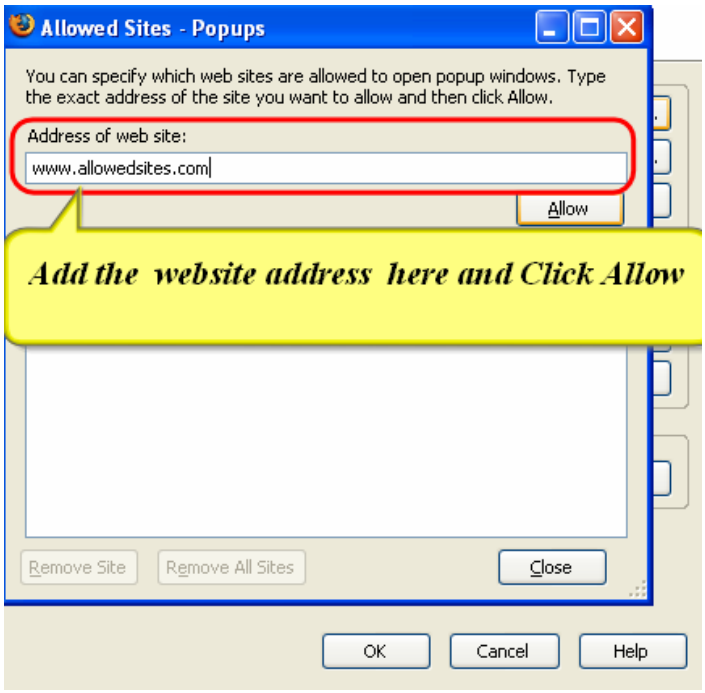


2. Check the '**Block pop-up windows**' check box



3. Click on the '**Exceptions**' button to add a few websites from whom pop-ups may be allowed.

4. Type the address of the website that you want to allow and click 'Add' button



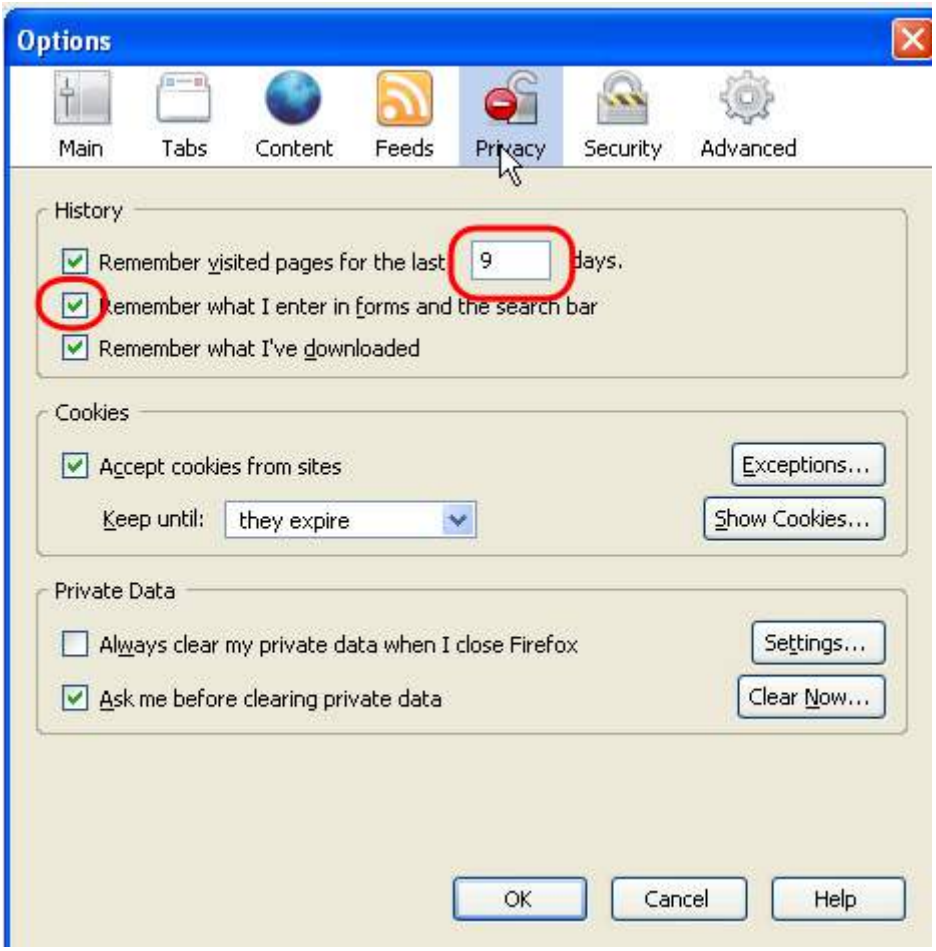
JavaScript Control:

JavaScripts are used to provide the active content of a website. Since they are based on the principle of triggering a piece of program depending on the user input, they execute the moment a user clicks or inputs some data anywhere in the page. This is one of the methods used by malicious code programmers to get into a system and thus poses a threat.

Firefox allows for the control of the JavaScript execution. Click on the **'Tools|Options'** menu item and then click on the **'Content'** tab and check the 'Enable JavaScript' check box. The default setup provided by Firefox should offer sufficient functionality and need not be worried about to tinker with.

History:

The access to the settings of the history of pages visited is held in the '**Privacy**' tab of the Firefox options. It is advised to change the '**Remember visited pages for the last ___ days**' box to a **0 (zero)** value.

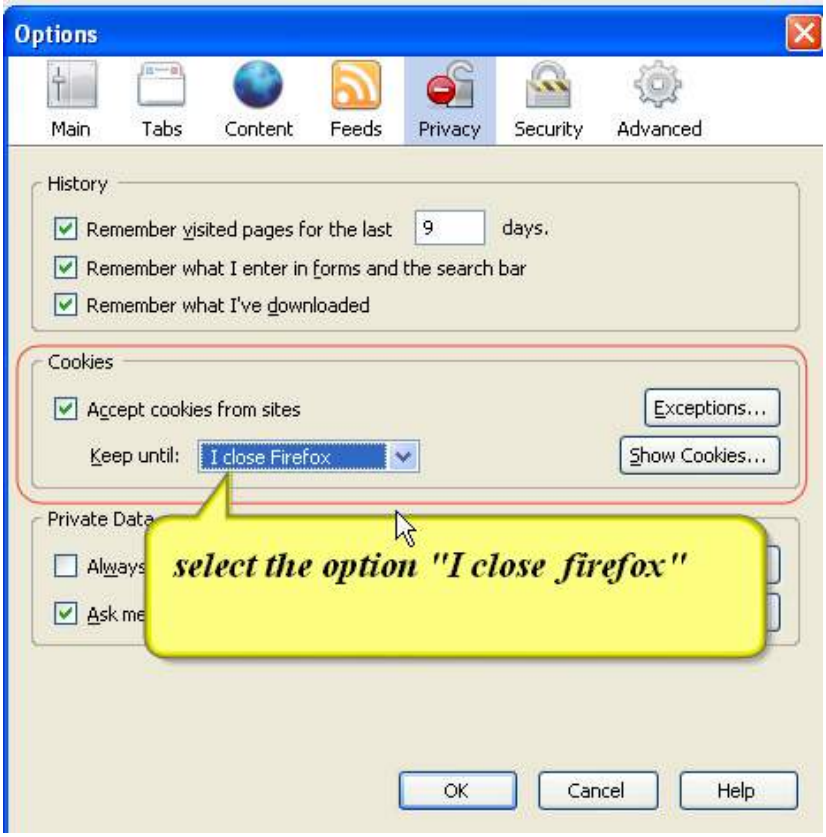


Uncheck the '**Remember what I enter in forms and the search bar**' box. This guarantees that none of your searches are stored in your cache that may be accessed by someone else.

Cookies:

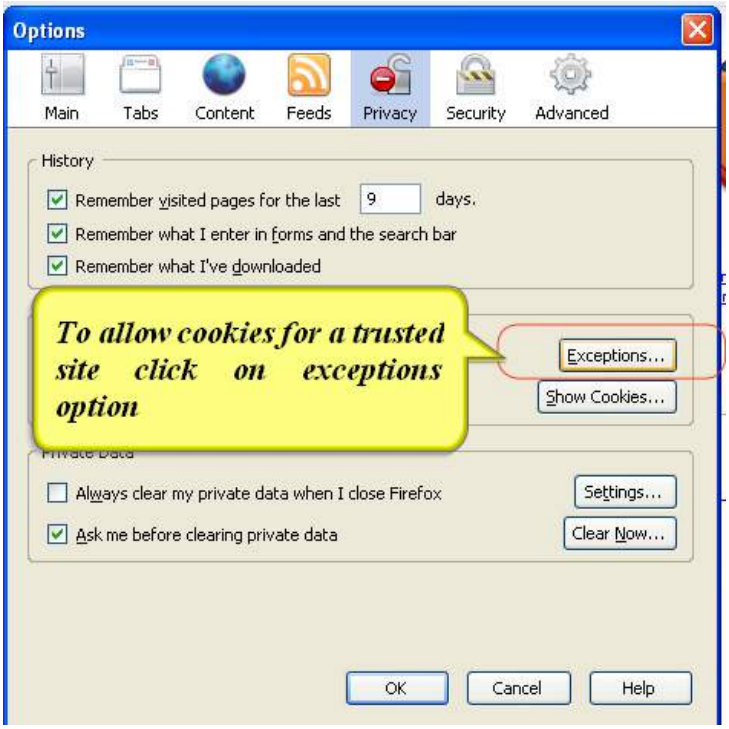
Firefox offers control of cookies by allowing the user the choose whether or not to accept cookies at all. A user may choose the '**Exceptions**' and then choose to either allow, temporarily allow or block cookies from a website. This setting is offered irrespective of the user's choice to allow/disallow a cookie. User discretion is advised here to allow or cookies at all and then give selective accept/deny to cookies.

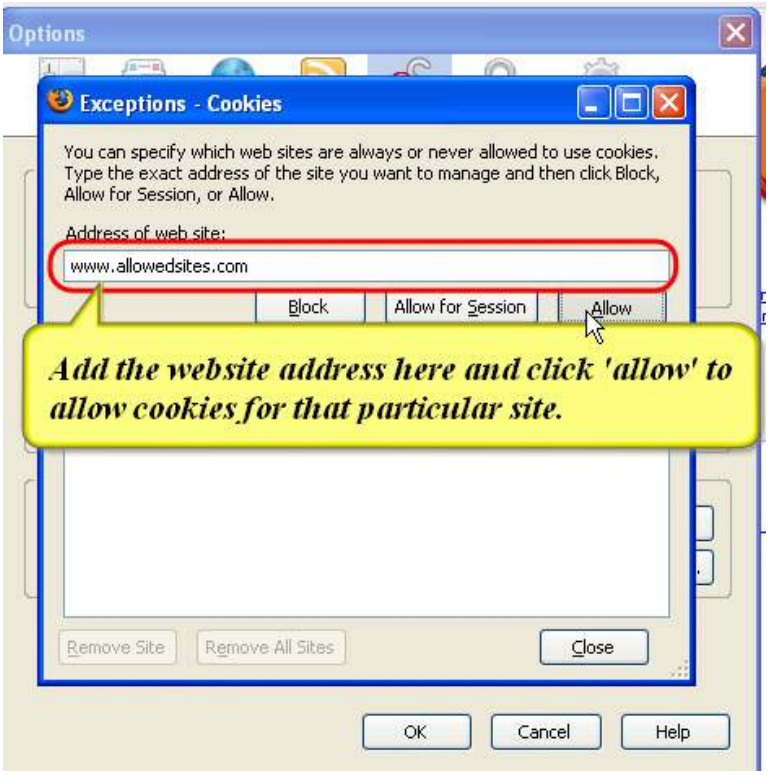
1. Access to the cookies settings can be found in the '**Privacy**' tab of the Firefox options.



2. Select the option 'I close Firefox' to not to accept cookies in the next session.

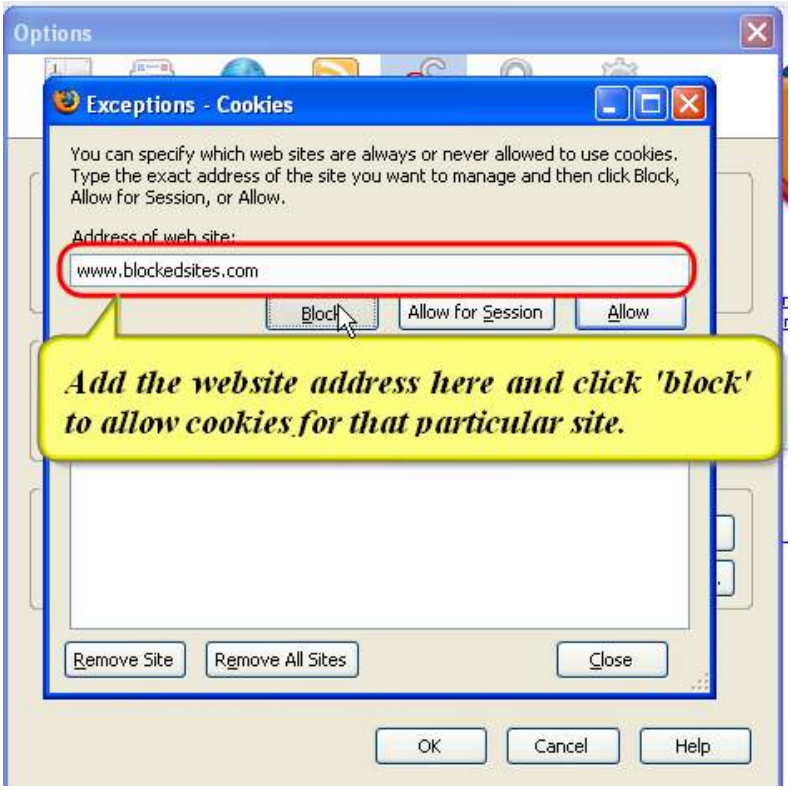
3. You can allow cookies for the trusted sites by clicking the 'Exceptions' tab.





4. Type the website that you want to allow and click 'Allow' button.

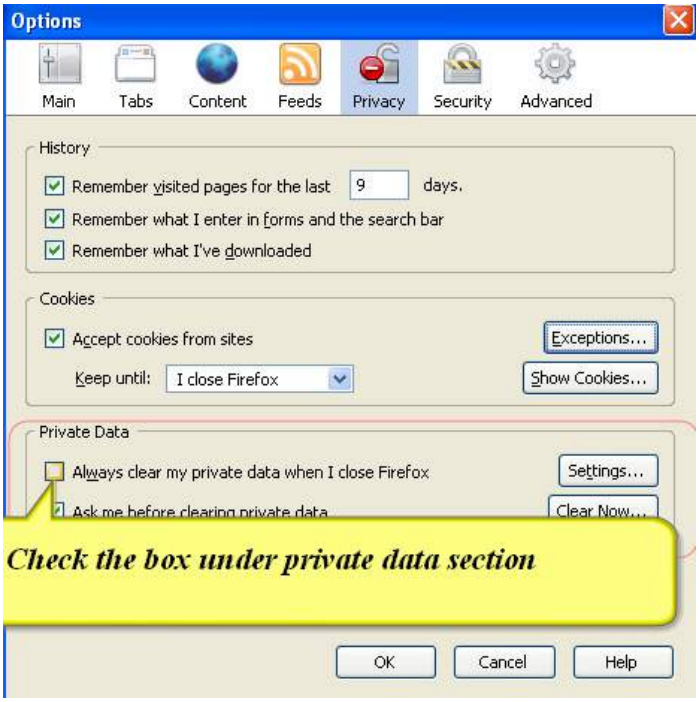
5. Type the website that you want to block, and click 'Block' button

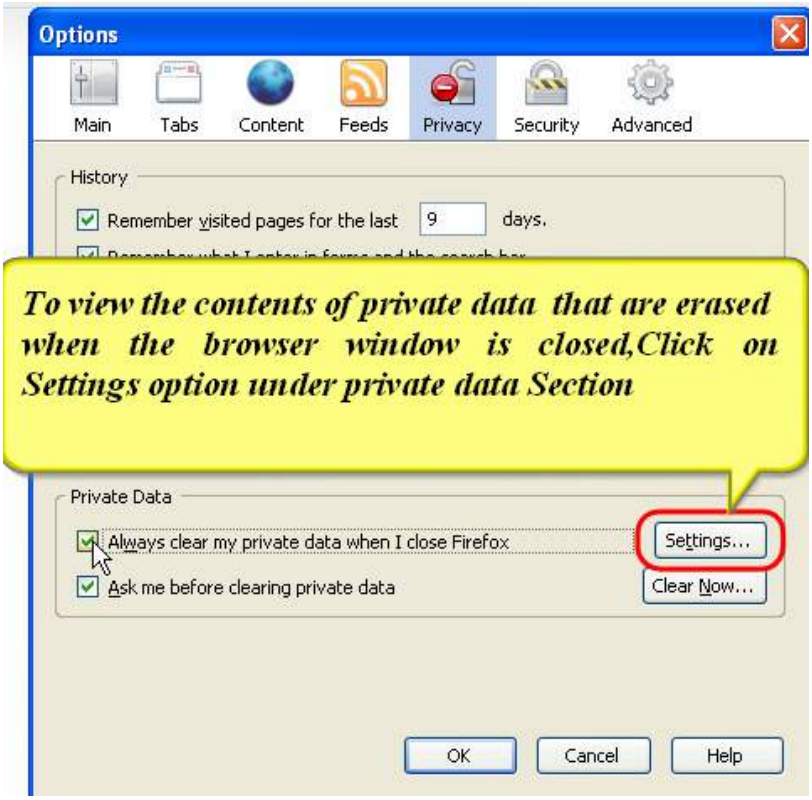


Private Data

1.Firefox allows you to clear all private data, Browsing History, Download History, Saved Forms Information etc automatically every time you close a session rather than you manually doing it.

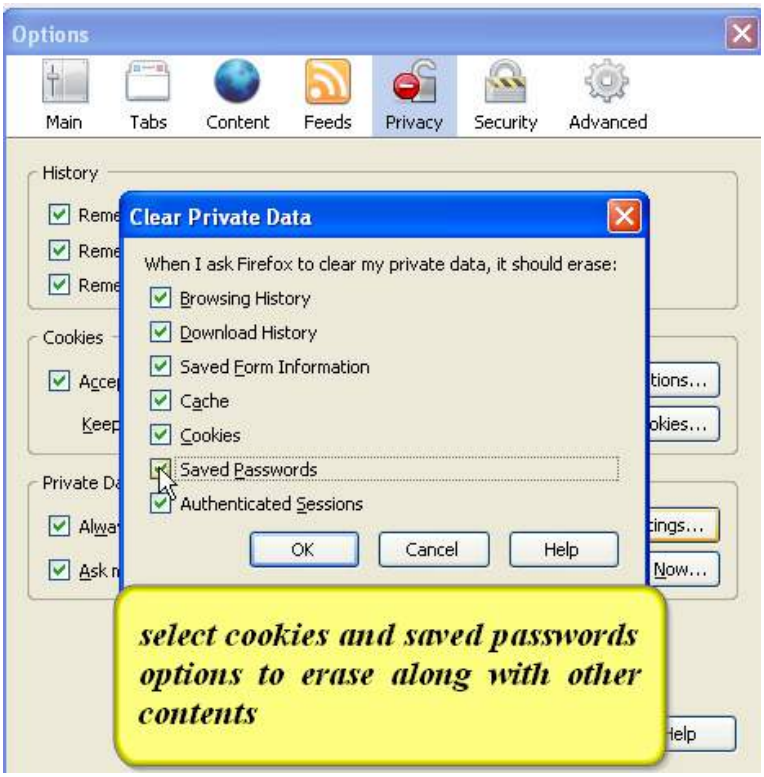
- Click '**Tools|Options**' menu item and then click the '**Privacy**' tab.
- Under the '**Private Data**' section, check the 'Always clear my private data when I close Firefox' check box.



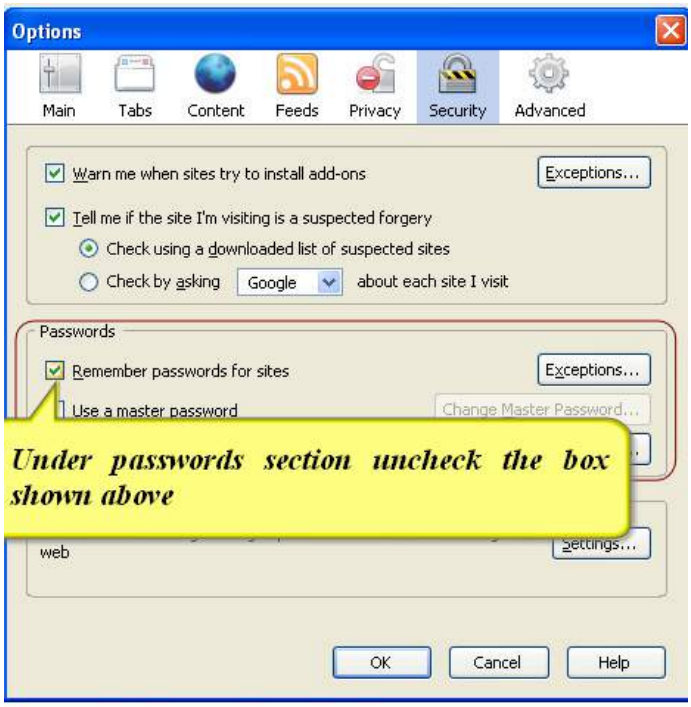


2. To view what are all contents that are erased when the browsing window is closed, click settings button.

3. Select 'Cookies and saved passwords'.



4. To avoid storing of user passwords by the browser, Click security tab.



5. Uncheck the box as shown below.

The 'Settings' control offer you the control of what gets deleted upon every exit. Remember to check the cookies to be cleared.

However, whether or not to clear the saved passwords depends on the user's preference to use the Password Manager facility. The 'Ask me before clearing private data' option prompts you to decide to clear private data at session close. A check mark indicates a prompt each time the session close.