**Branch :- Computer Sci. & Engg. Class :- Final Year**

**Subject :-System and Software Security Lab manual Sem :- VII**

**Teacher Manual**

**PRACTICAL NO 08**

**Practical no. 2**

**AIM**:- Propose steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome).

**S/W REQUIRED:-** Mozilla Firefox/Google Chrome

**THEORY:-**

Browser security is an important part in keeping your information safe.

Your browser is the window to the internet and also the first line ofdefence against malware threats. Some small tweaks to your browser security settings are all that you need to make your time online that much

safer.

**Browser features and their security vulnerabilities**

Browsers use many tools for various tasks, such as Java, Flash Player,ActiveX, etc. But these often come with security flaws, which cybercriminals exploit to get access to your PC. A quick rundown of these tools will help you figure out if you need them or not.

**Deactivate ActiveX**. A browser add-on that comes preinstalled on Internet Explorer or Microsoft Edge and only works with these browsers. ActiveX acts as a middle man between your PC and Java/Flash based interactions in certain sites. This creates security problems by giving malicious websites a window into

your PC. What’s more, ActiveX is rarely used nowadays, so be on your guard if a site asks you to install it and accept the installation only if you are 150% sure that site is trustworthy.

**Try to disable JavaScript.** JavaScript is a programming language used by websites to run various programs and features. Sites such as YouTube or Google Docs need it to function, but so do advertising, pop-up software and a whole host of other spammy elements from the internet.

Cyber-criminals use JavaScript in malicious ways in order to infect your device with malware and other harmful software.

If you disable JavaScript altogether you will get a much quicker and simplified browser experience, with little to no ads, pop-ups, greatly improved page load times and generally a cleaner Internet experience at the

cost of specialized tools such as Google Docs or YouTube.

This doesn’t need to be as drastic as it sounds, since browsers do allow you to white list certain sites which can run JavaScript.

**Delete Cookies.** These are small data files stored on your browser. Websites use cookies in order to remember your accounts and passwords, browsing history and to track user behaviour on their site.

Because of the information they contain, cookies are prime targets for cybercriminals, especially the ones that contain emails, account names and passwords.

When you disable and clear cookies you cut down on the personal data cybercriminals can obtain.

One thing you will want to keep in mind is that there are **two types of**

**cookies:**

First party and third party cookies. First party cookies are placed by the site you visit, for instance you get a first party cookie by cnn.com while visiting cnn.com.

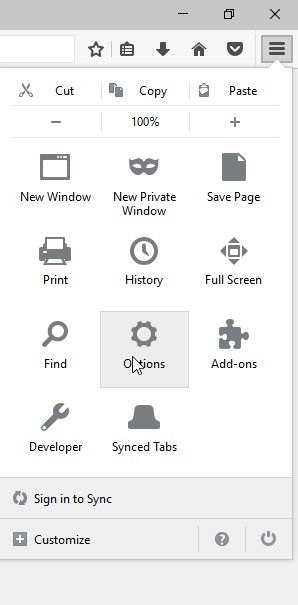
Third party cookies are placed by other sites, for example you get a cookie from amazon.com while visiting cnn.com.

First party cookies are frequently used to remember your login information so you don’t have to enter it every time you visit a site. But we can’t stress this enough, **don’t allow your browser to save passwords.**

Third party cookies are almost always placed on your computer by advertisers or marketers interested in tracking your movement online, so nothing bad will happen if you block them.

**Browser extensions and add-ons** add extra functionality to your browser such as ad blocking or search bars. However, these add-ons pose a security risk, since they can open up windows into your PC which can be exploited to inject malware.

**Firefox hacks and tips for better security**

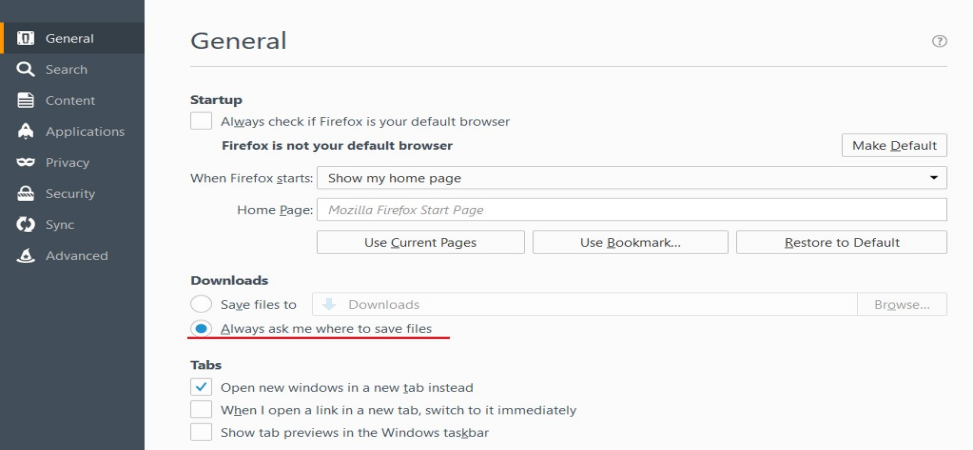


If you use Mozilla Firefox and want to improve your browser security settings, press the hamburger menu in the top right corner and go to “Options”.

In the “General” tab, at the Downloads section, press “Always asks me where to save files”. This way, you won’t have a web location try to automatically save dangerous content to your computer. At the same time,

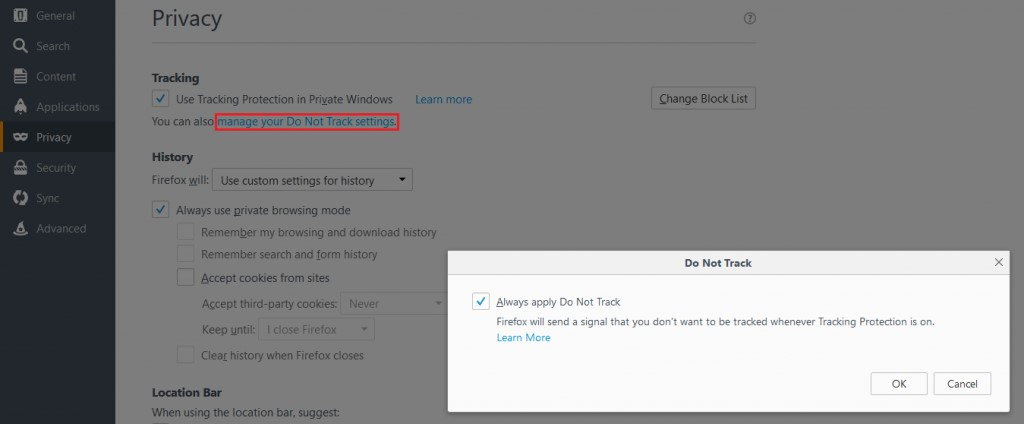
this gives you the option to place suspicious content in a safe location where

you can analyze it afterwards.

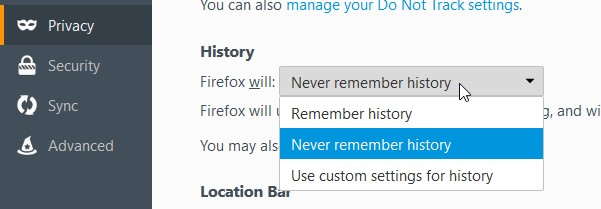


Next, go to **the Privacy tab.**

At the “Tracking” section press the blue text with “manage your Do Not Track settings” and check “Always apply do not track”. After you do this advertising, commerce and various other sites shouldn’t be able to track you across the web.

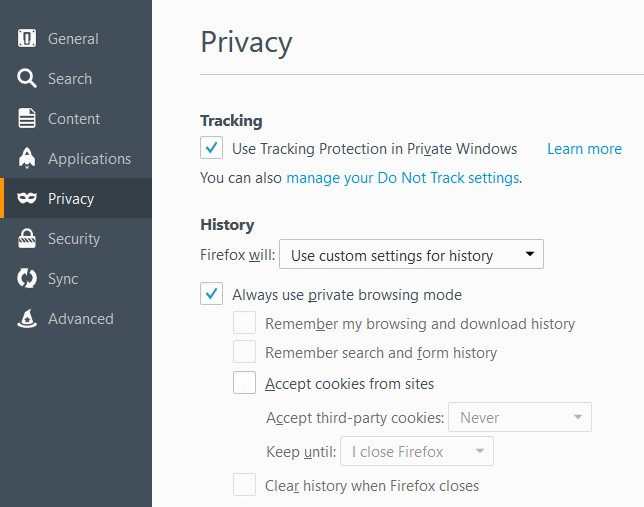


While in the Privacy tab, at the “History” section, choose “Firefox will never remember history”. This is especially important if you know your device may be used by other people.



For a more detailed control of your history section, select “Use custom

settings for history”.



Check “Always use private browsing mode” so every time you close your Firefox browser it will clear browsing history, search results, cookies and download history.

The last changes you should make in Firefox can be found in the “Security”

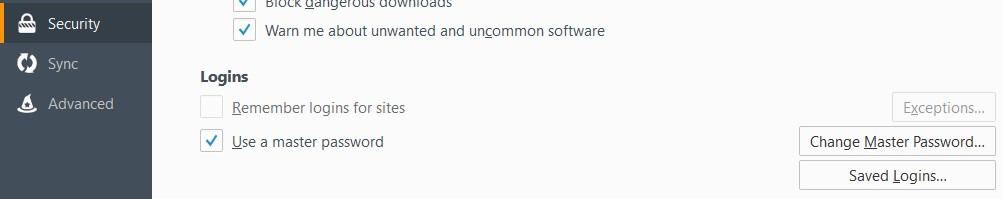
category.



First, make sure all of the four check boxes in the General section are checked in. This ensures that your browser will inform you whenever websites try to install malicious add-ons and other content.

In the “Logins” section you can set up a Master Password. Doing this is especially useful when multiple people have access to the computer, since it asks you introduce a master password before you can access logins.

This way, other people won’t be able to access your important accounts such as email. Once more, we cannot recommend this enough, but don’t let your browser remember your passwords.



**CONCLUSION:** Thus, we have proposed steps to ensure Security of web browser.