LAB 5

Instruction: Please answer all the questions

Activity 1: Configure Microsoft Windows Data Execution Prevention (DEP)

Data Execution Prevention (DEP) is a Microsoft Windows feature that prevents attackers from using buffer overflow to execute malware. Most modern CPUs support an NX (No eXecute) bit to designate a part of memory for containing only data. An attacker who launches a buffer overflow attack to change the "return address" to point to his malware code stored in the data area of memory would be defeated because DEP will not allow code in the memory area to be executed. If an older computer processor does not support NX, then a weaker software-enforced DEP will be enabled by Windows. Software-enforced DEP protects only limited system binaries and is not the same as NX DEP. DEP provides an additional degree of protection that reduces the risk of buffer overflows. In this project, you will determine if a Microsoft Windows system can run DEP. If it can, you learn how to configure DEP.

Lab Steps:

1. The first step is to determine if the computer supports NX. Use your Web browser to go to www.grc.com/securable. Click Download now and follow the default settings to install the application on your computer.
2. Double-click SecurAble to launch the program. If it reports that Hardware D.E.P. is "No," then that computer's processor does not support NX. Close the SecurAble application.
3. The next step is to check the DEP settings. Click Start and Control Panel.
4. Click System and Security and then click System.
5. Click Advanced system settings in the left pane.
6. Click the Advanced tab.
7. Click Settings under Performance and then click the Data Execution Prevention tab.
8. Windows supports two levels of DEP controls: DEP enabled for only Windows programs and services and DEP enabled for Windows programs and services as well as all other application programs and services. If the configuration is set to Turn on DEP for essential Windows programs and services only, then click Turn on DEP for all Windows programs and services except those I select. This will provide full protection to all programs.

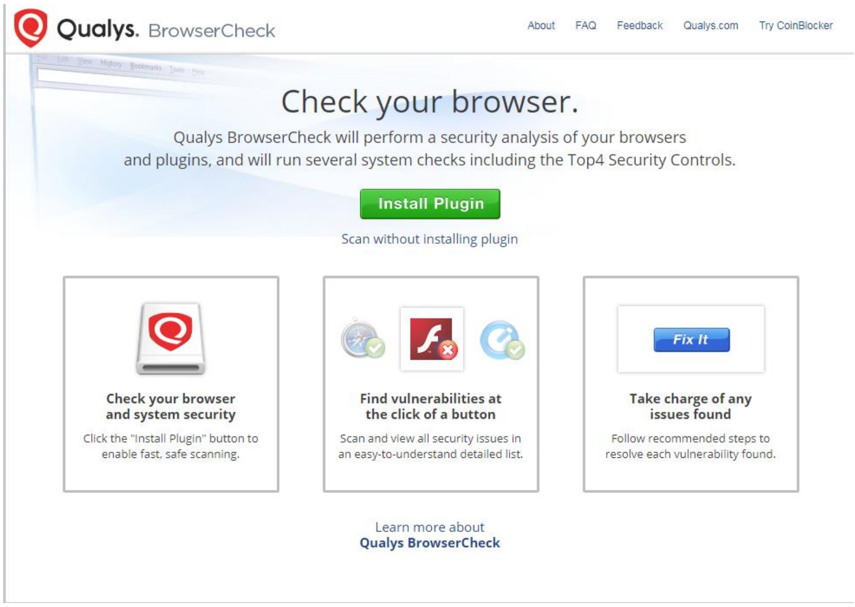
9. If an application does not function properly, it may be necessary to make an exception for that application and not have DEP protect it. If this is necessary, click the Add button and then search for the program. Click the program to add it to the exception list.
10. Close all windows and applications and then restart your computer to invoke DEP protection.

Question:

1. Explain the relationship between buffer overflow and Data Execution Prevention.
2. Is there a need to turn "ON" Data Execution Prevention setting? Explain why.

Activity 2: Explore Web Browser Security

1. Go to https://browsercheck.qualys.com/
2. The Qualys browsercheck website is displayed as shown below



Check your browser.

Qualys BrowserCheck will perform a security analysis of your browsers and plugins, and will run several system checks including the Top4 Security Controls.

Scan without installing plugin

Check your browser and system security

Click the "Install Plugin" button to enable fast, safe scanning.

Find vulnerabilities at the click of a button

Scan and view all security issues in an easy-to-understand detailed list.

Take charge of any issues found

Follow recommended steps to resolve each vulnerability found.

Learn more about **Qualys BrowserCheck**

3. Click 'Scan without installing plugin'
4. Click 'Scan Now'
5. Check the box of 'Service User Agreement' and continue
6. The results of web browser plug-in will display

7. Re-conduct this scanning in different web browser platform.

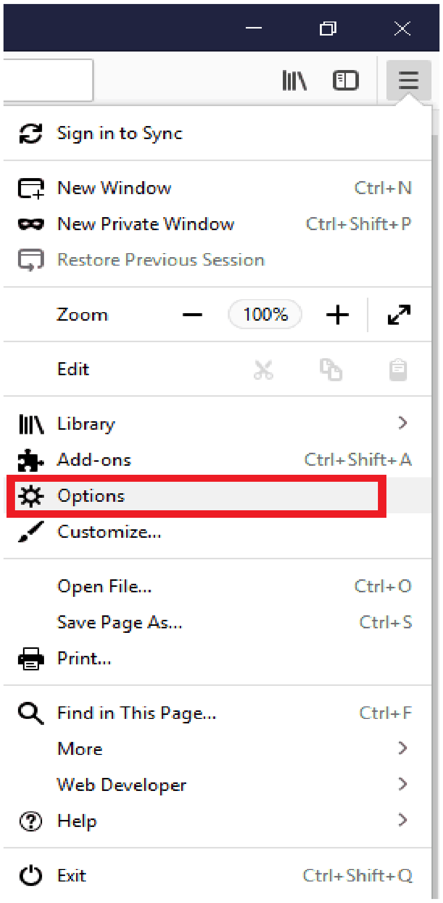
Question:

3. Why web browser plug-in need to constantly update?

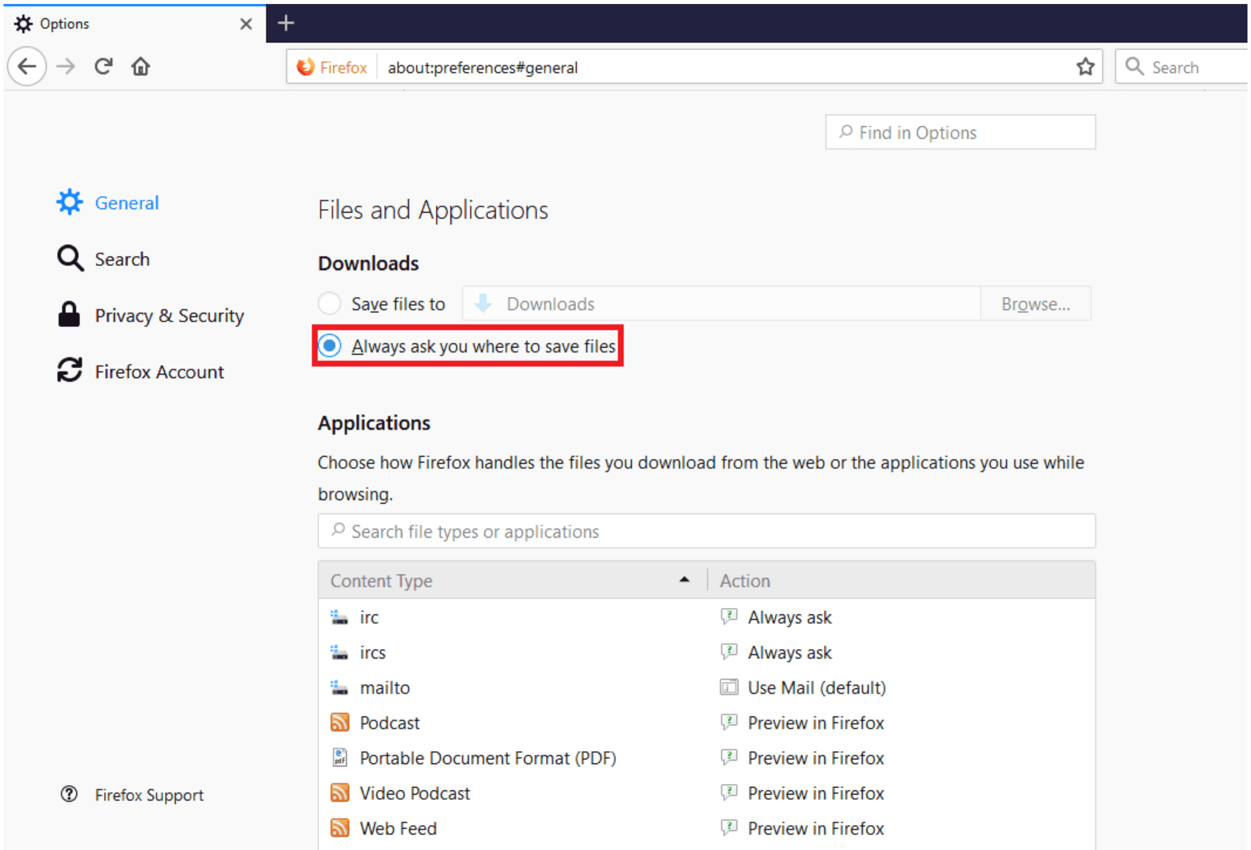
Activity 3: Explore Web Browser Security - Security Settings to Use for Firefox, Chrome, and Explorer

4.1 How to Secure Firefox?

1. To edit the security settings on Firefox, click the top right menu and select ***Options***.



2. In the ***General*** section, select ***Always ask you where to save files*** to prevent malicious attachments and files from automatically being downloaded on your computer.



Files and Applications

Downloads

○ Save files to Downloads Browse...

● Always ask you where to save files

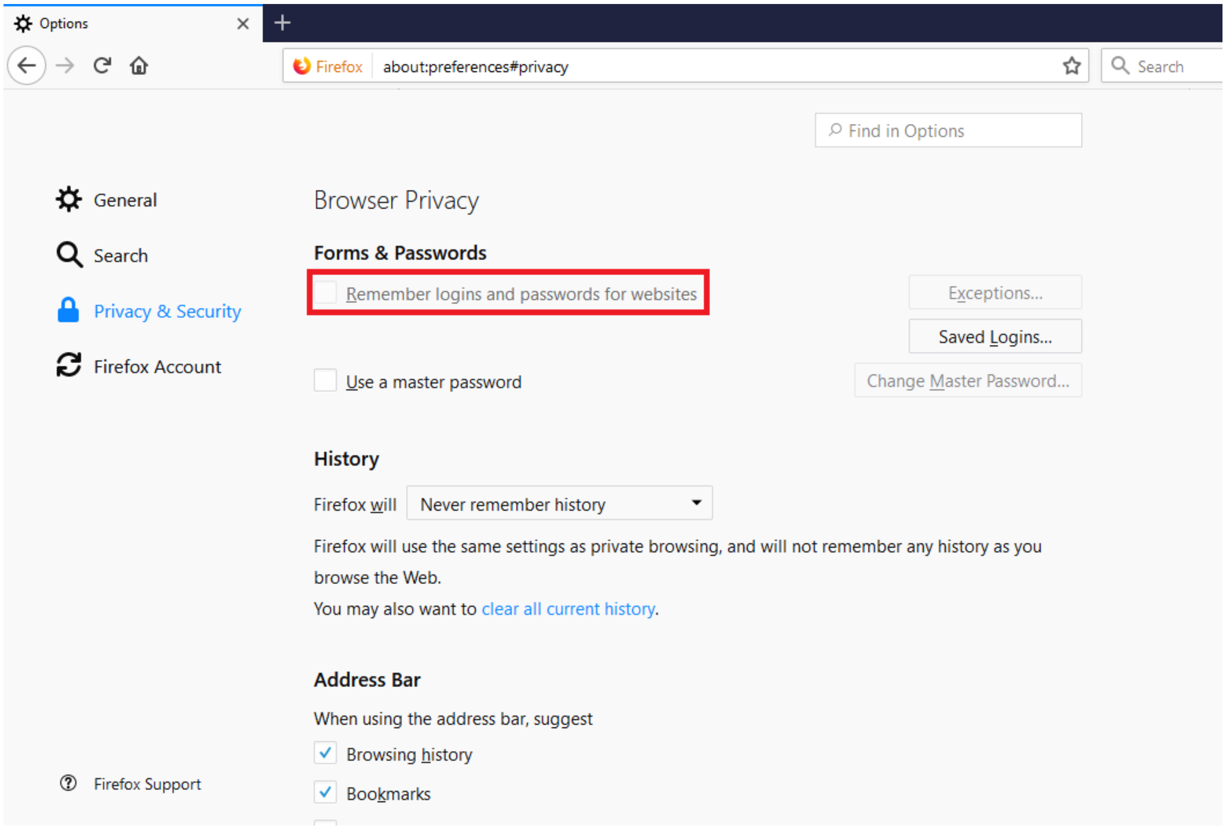
Applications

Choose how Firefox handles the files you download from the web or the applications you use while browsing.

Search file types or applications

Content Type	Action
irc	Always ask
ircs	Always ask
mailto	Use Mail (default)
Podcast	Preview in Firefox
Portable Document Format (PDF)	Preview in Firefox
Video Podcast	Preview in Firefox
Web Feed	Preview in Firefox

3. Go to the ***Privacy & Security*** section and uncheck ***Remember logins and passwords for websites***. It means that you'll have to enter this information manually every time, but according to cybersecurity experts, autofill passwords can make it a whole lot easier to get hacked – thus making this an important browser security practice**.**



Browser Privacy

Forms & Passwords

□ Remember logins and passwords for websites

□ Use a master password

History

Firefox will: Never remember history

Firefox will use the same settings as private browsing, and will not remember any history as you browse the Web.

You may also want to clear all current history.

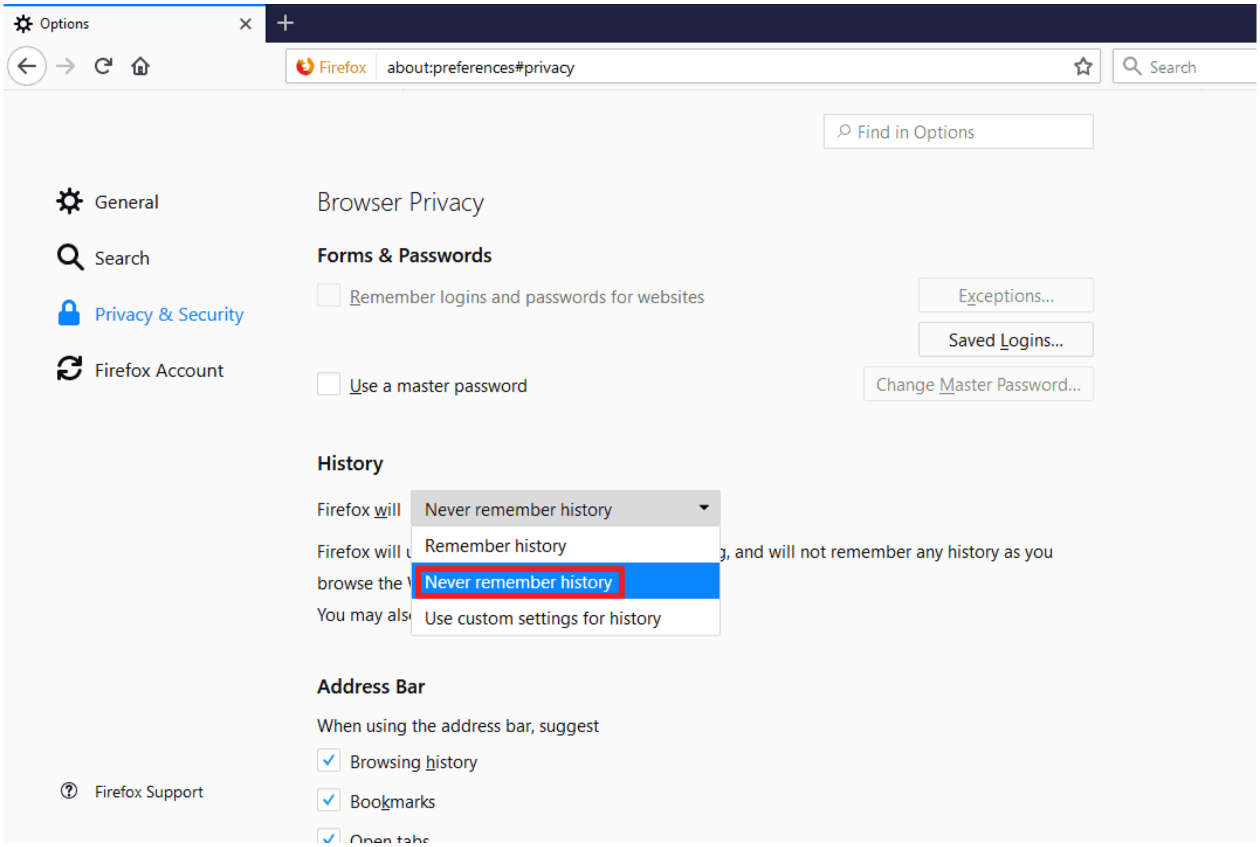
Address Bar

When using the address bar, suggest

☑ Browsing history

☑ Bookmarks

4. If your computer is used by multiple people, change ***Firefox will: Remember history*** to ***Firefox will: Never remember history*** from the ***Browser Privacy*** category**.** You’ll be prompted to restart Firefox once you enable this feature. Click ***Restart Firefox now*** to validate.



Browser Privacy

Forms & Passwords

□ Remember logins and passwords for websites

□ Use a master password

History

Firefox will Never remember history

- Remember history
- Never remember history
- Use custom settings for history

Firefox will u , and will not remember any history as you browse the

You may als

Address Bar

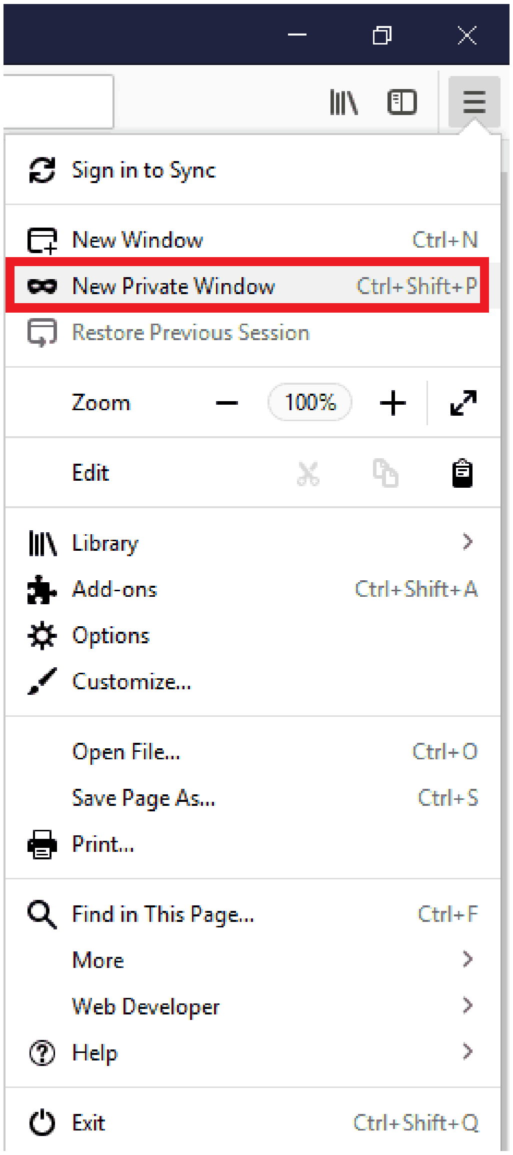
When using the address bar, suggest

☑ Browsing history

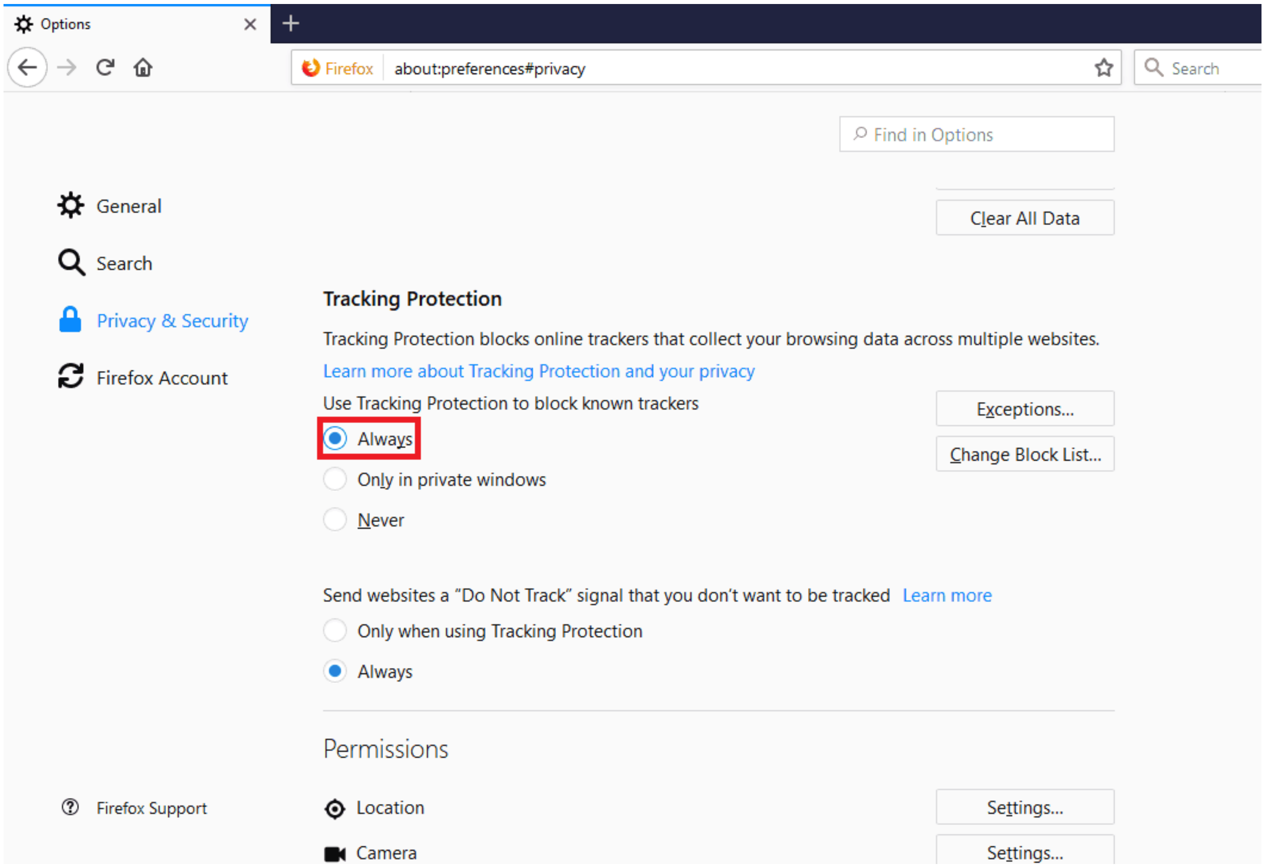
☑ Bookmarks

☑ Open tabs

Note: You can also use the Private Browsing mode for this purpose. Simply select ***New Private Window*** from the top right menu or use the keyboard shortcut ***Ctrl+Shift+P***.



5. Now, set ***Tracking Protection*** to ***Always*** so that websites can’t track you across the Internet and collect your browsing data.



Tracking Protection

Tracking Protection blocks online trackers that collect your browsing data across multiple websites.

Learn more about Tracking Protection and your privacy

Use Tracking Protection to block known trackers

● Always

○ Only in private windows

○ Never

Send websites a "Do Not Track" signal that you don't want to be tracked Learn more

○ Only when using Tracking Protection

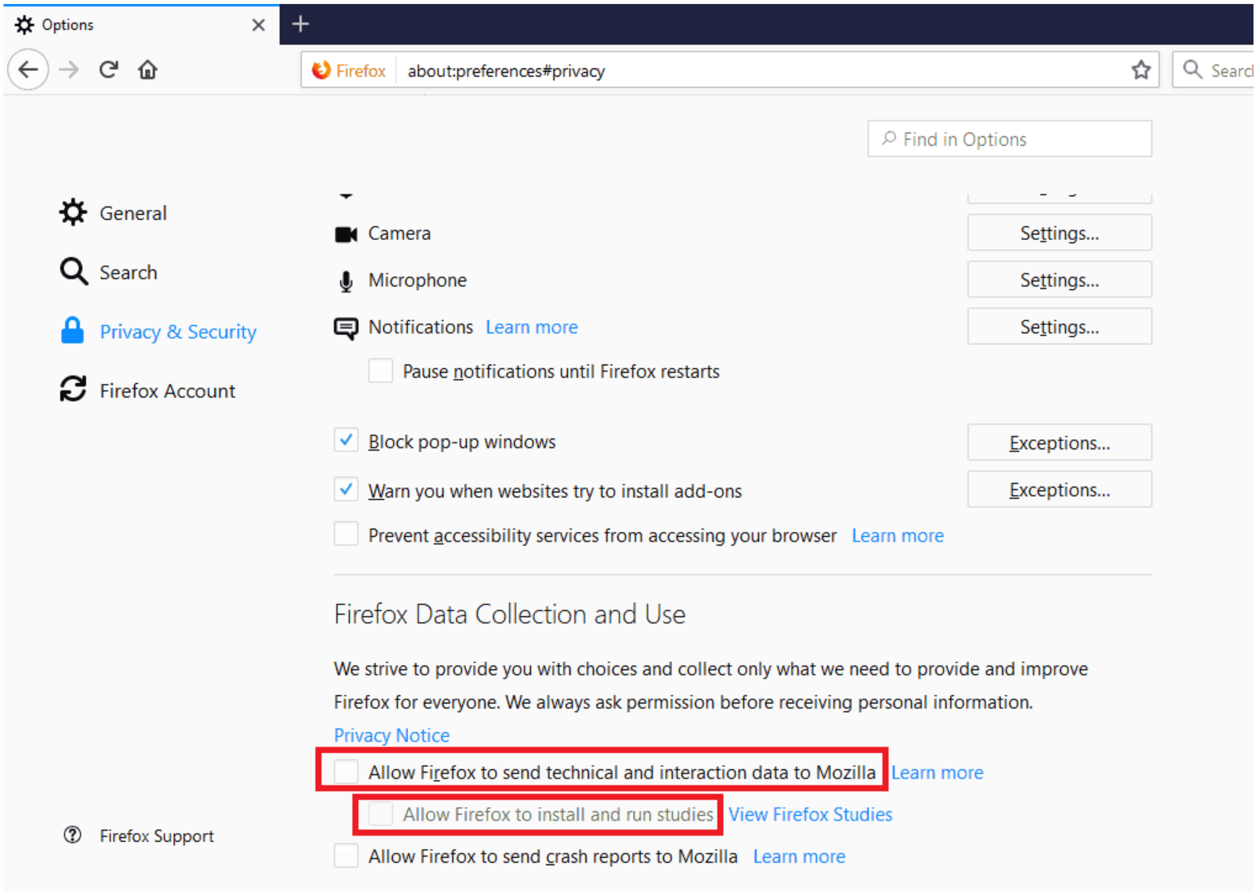
● Always

Permissions

Location

Camera

6. Uncheck the first two boxes under ***Firefox Data Collection and Use*** to opt out of sharing data with Firefox.



Camera

Microphone

Notifications Learn more

☐ Pause notifications until Firefox restarts

☑ Block pop-up windows

☑ Warn you when websites try to install add-ons

☐ Prevent accessibility services from accessing your browser Learn more

Firefox Data Collection and Use

We strive to provide you with choices and collect only what we need to provide and improve Firefox for everyone. We always ask permission before receiving personal information.

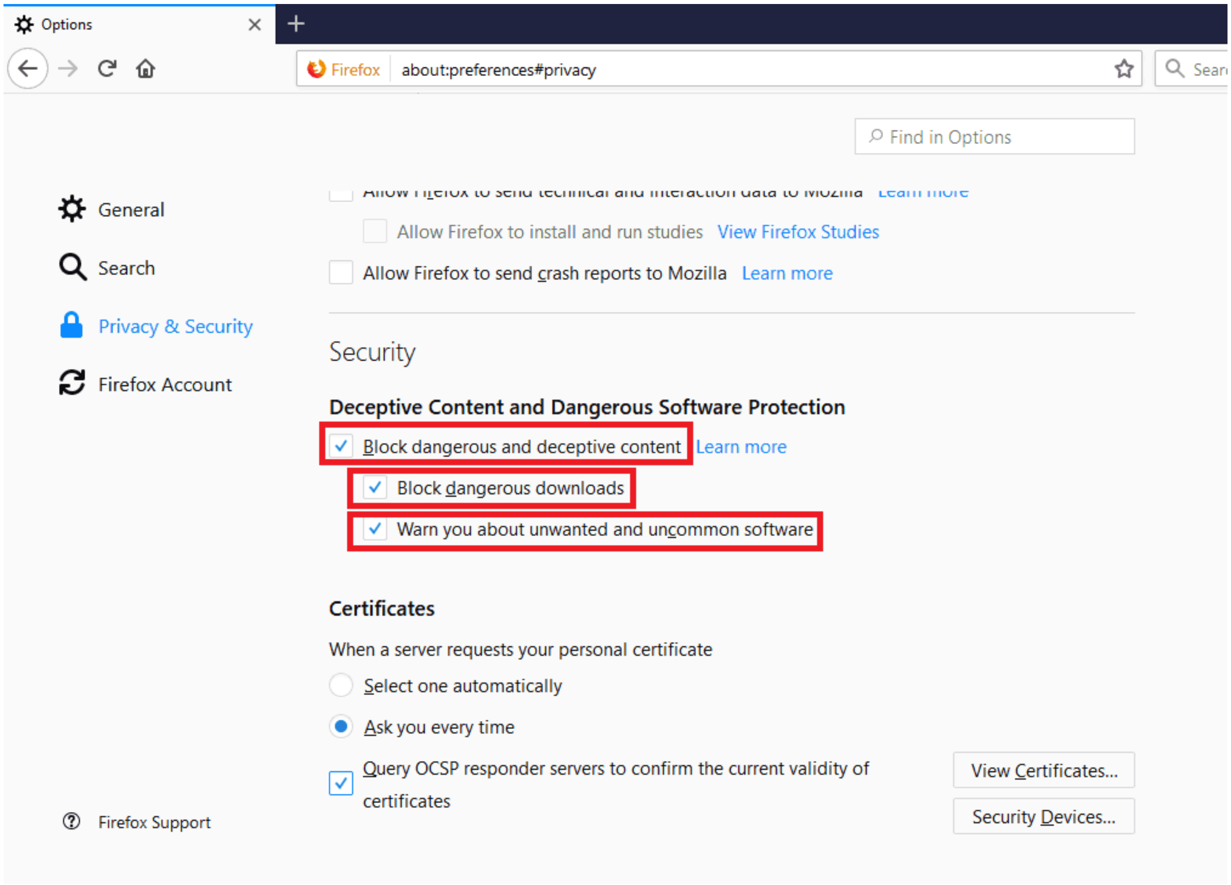
Privacy Notice

☐ Allow Firefox to send technical and interaction data to Mozilla Learn more

☐ Allow Firefox to install and run studies View Firefox Studies

☐ Allow Firefox to send crash reports to Mozilla Learn more

7. Lastly, check all the boxes under ***Deceptive Content and Dangerous Software Protection*** from the ***Security*** category. This ensures that you're informed by the browser whenever a website attempts to install malicious software or display dangerous content.



□ Allow Firefox to send technical and interaction data to Mozilla Learn more

□ Allow Firefox to install and run studies View Firefox Studies

□ Allow Firefox to send crash reports to Mozilla Learn more

Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

When a server requests your personal certificate

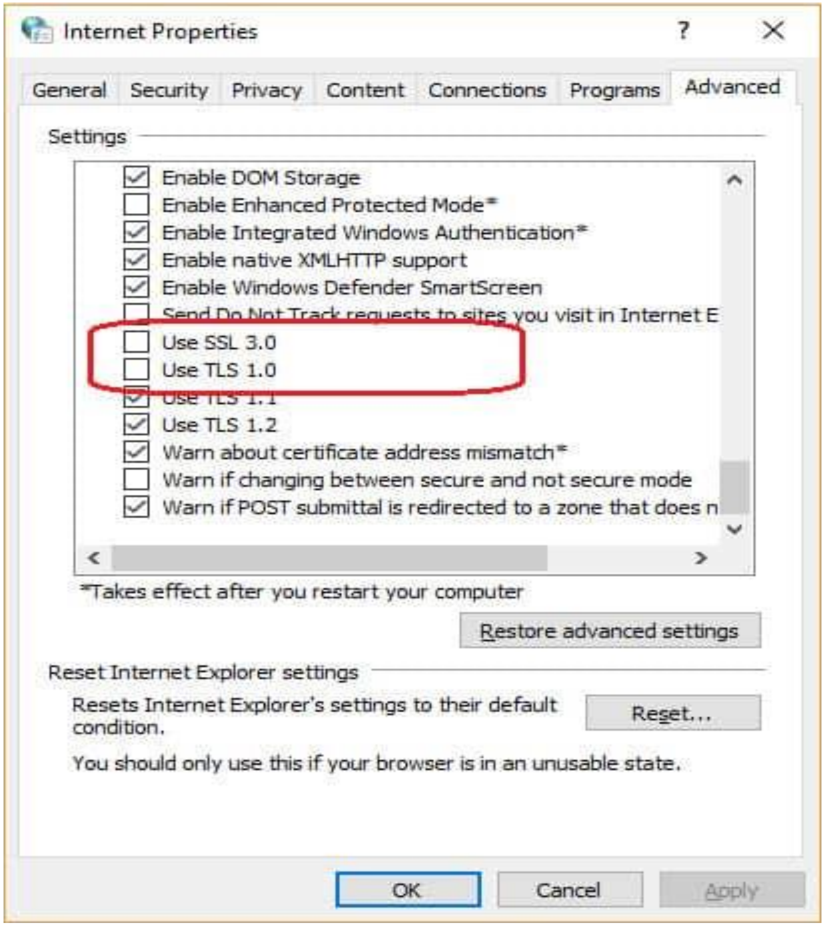
○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

4.2 How to Secure Chrome?

1. Click on the three dots symbol at the end of the address bar. In the drop-down menu select **Settings**. This will open a new tab.
2. Scroll down in the Settings screen to the bottom and click on **Advanced**. The screen will extend. Scroll down to find the **System** section and click on **Open proxy settings**. This will open the Internet Properties window.
3. Click on the **Advanced** tab and scroll down in the **Settings** window. Make sure that **Use SSL 3.0** and **Use TLS 1.0** are de-selected.



☑ Enable DOM Storage
☐ Enable Enhanced Protected Mode*
☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
☑ Enable Windows Defender SmartScreen
☐ Send Do Not Track requests to sites you visit in Internet E
☐ Use SSL 3.0
☐ Use TLS 1.0
☑ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate address mismatch*
☐ Warn if changing between secure and not secure mode
☑ Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart your computer

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

4. Click on **OK** in the Internet Properties window to save the changes.
5. Return to the Advanced Settings screen in Google Chrome and look for the **Privacy and security** section. Click on the arrow next to **Content settings**.
6. Click on the arrow next to **JavaScript** and in the next screen, click on the slider to turn it to **Blocked**. Click on the back arrow at the top of the JavaScript screen to return to Content Settings.

7. Click on the arrow next to **Flash** — this is the next entry down from the **JavaScript**setting. In the next screen, click on the slider so the message next to it reads **Block sites from running Flash**. Click on the back arrow at the top of the screen to get back to the Content Settings list.
8. Scroll down to **Popups** and click on the arrow in that line. Click on the slider so that you see that popups are blocked. Click on the back arrow at the top of the screen.
9. Scroll down to **PDF documents**, which is the next to last entry in the **Content Settings** list. Click on the arrow on that line. Click on the slider so that the message next to it reads **Download PDF files instead of automatically opening them in Chrome**.

Question:

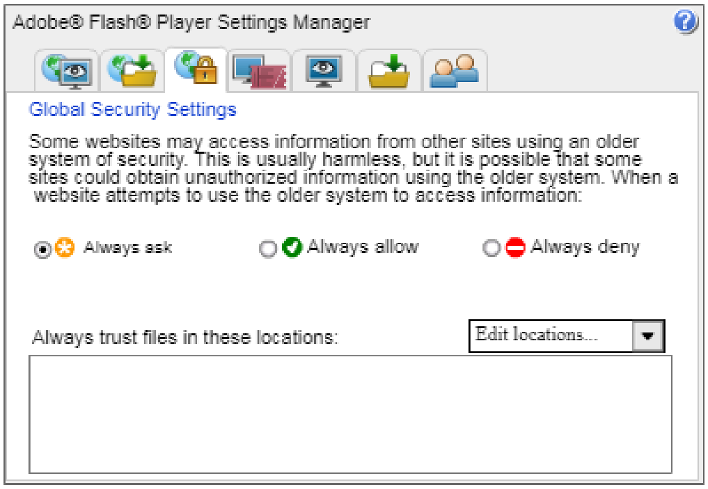
4. Why web browser security setting is important?
5. There's several types of security setting in web browser that you need to cater. Explain two settings and why this setting is important?

Activity 4: Manage Flash Cookies

Adobe Flash cookies are significantly different from regular cookies. Flash cookies can also be used to reinstate regular cookies that a user has deleted or blocked. Known as respawning, the deleted cookie's unique ID can still be assigned to a new cookie using the data stored in a Flash cookie as a backup. However, Flash cookies cannot be deleted through the browser's normal configuration settings as regular cookies can. Instead, they are managed through the Adobe Web site. In this project, you change the settings on Flash cookies.

1. Use your Web browser to go to https://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager02.html
2. The Global Privacy Settings panel is displayed as shown below

Global Security Settings panel



Adobe® Flash® Player Settings Manager

Global Security Settings

Some websites may access information from other sites using an older system of security. This is usually harmless, but it is possible that some sites could obtain unauthorized information using the older system. When a website attempts to use the older system to access information:

● Always ask ○ Always allow ○ Always deny

Always trust files in these locations: Edit locations... ▼

4. Click all tab: Global Privacy Settings, Global Storage Settings, Global Security Settings, Website Privacy Settings, Website Storage Settings and Peer-Assisted Networking panel.

Question:

6. For each tab panel, state your choice of settings. Explain why you choose that setting.