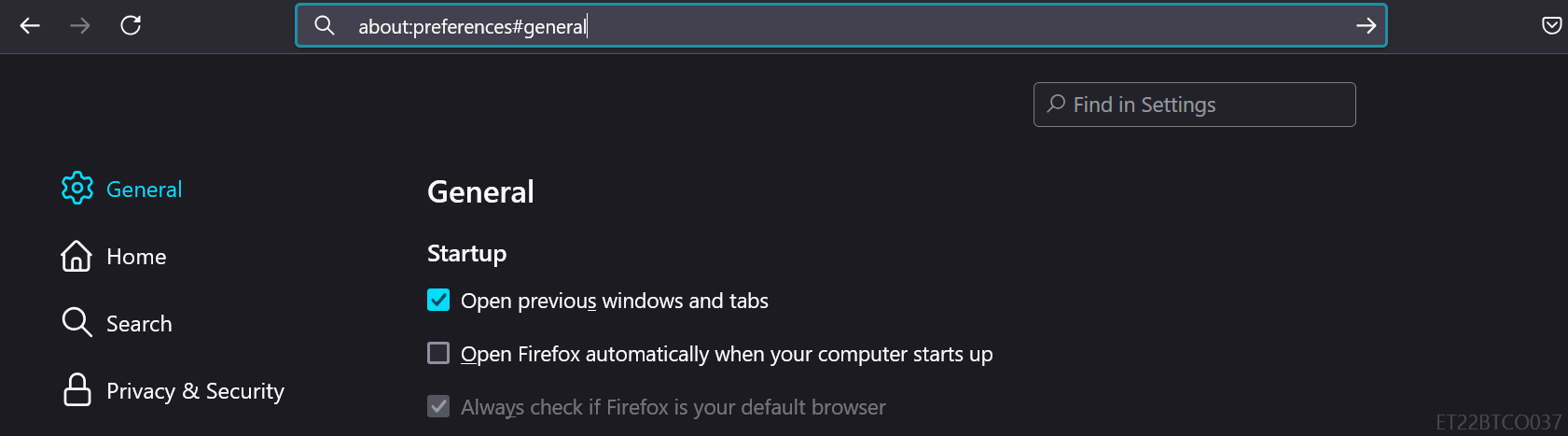
**Practical No : 11**

**Problem Statement:**

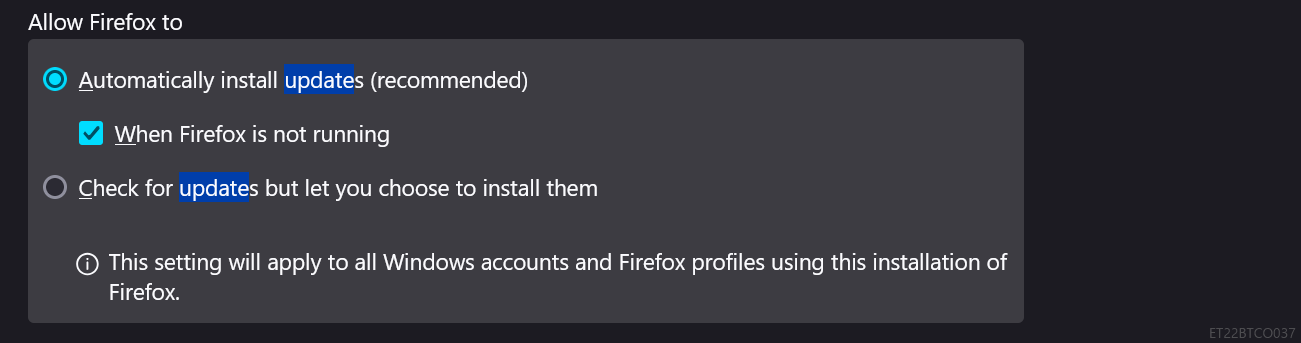
Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome)

**Steps:**

**Setting the default browser -** For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) > General tab. Check the box “Always check to see if Firefox is default browser on startup”.

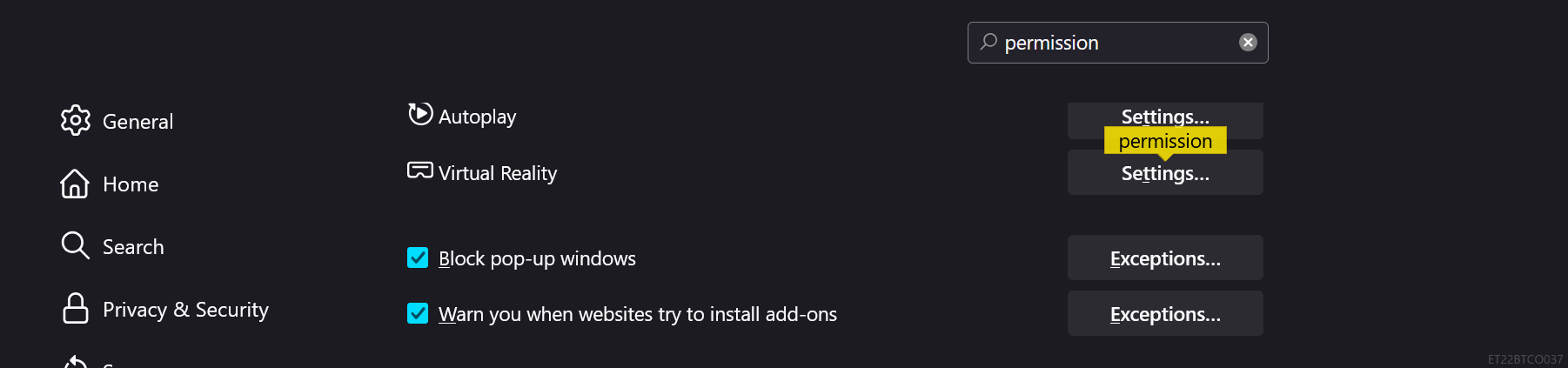


**Auto-install updates** - For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) General tab > Firefox Updates section. Select "Automatically install updates (Recommended)".

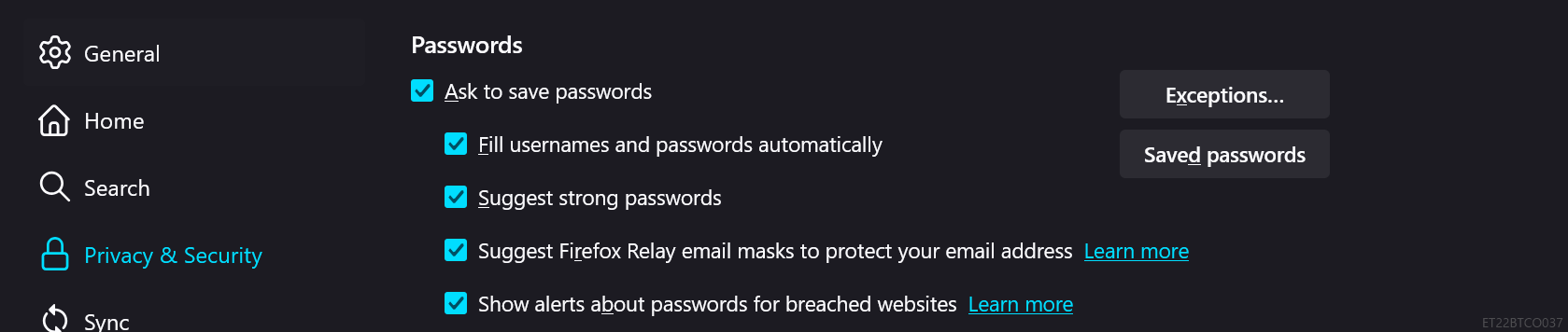


**Block unwanted pop-ups** - For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) > Privacy & Security > Permissions section. Check "Block pop-up windows".

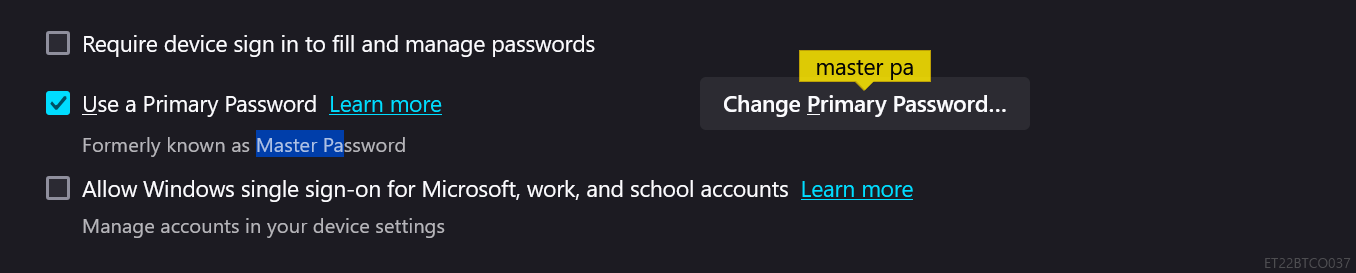
**Block unwanted add-ons** - For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) > Privacy & Security > Permissions section. Check "Warn you when websites try to insall add-ons".



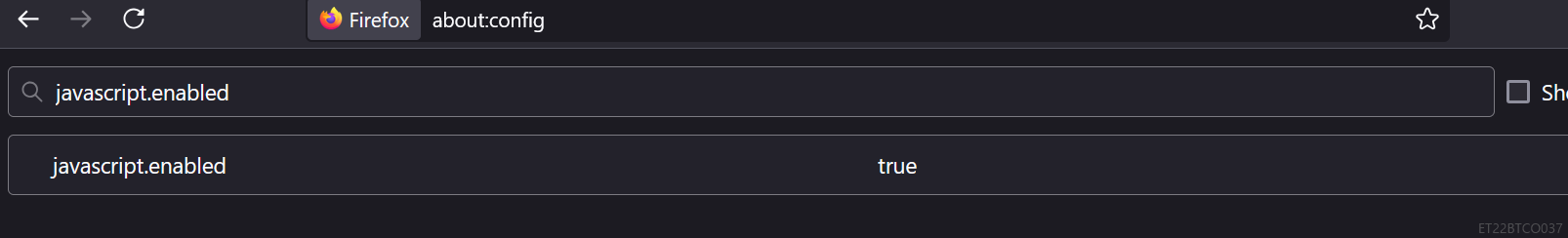
**Don't save passwords** - For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) > Privacy & Security > Browser Privacy section. Uncheck the "Ask to save logins and passwords for websites" box.



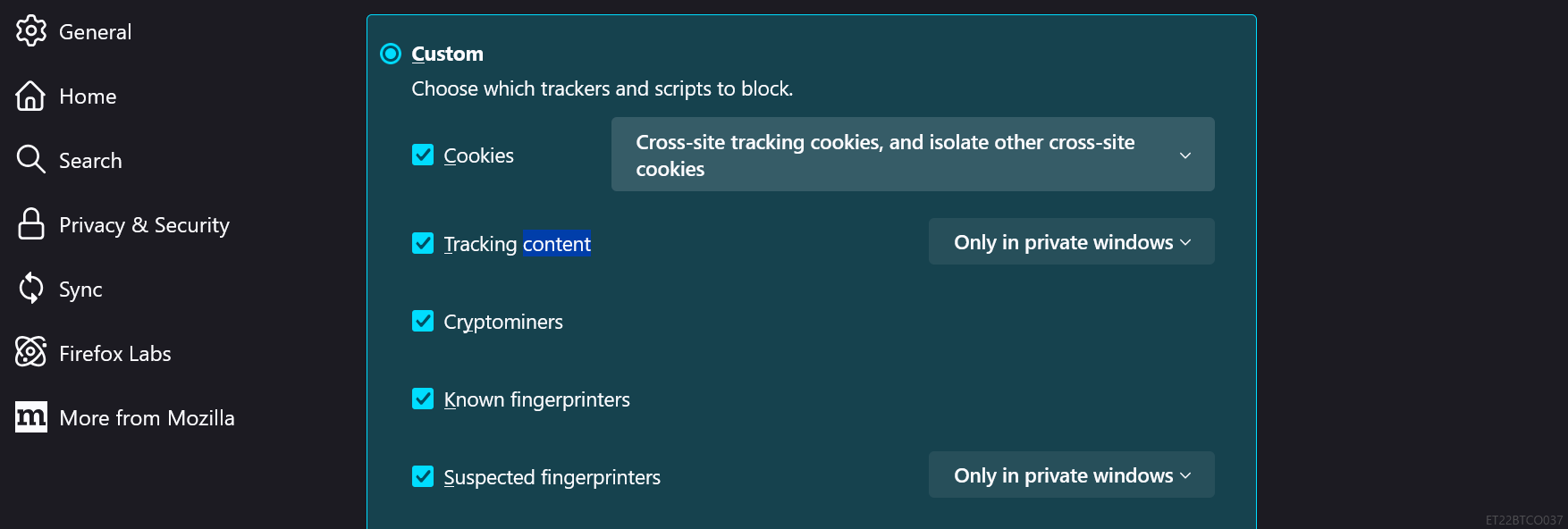
**Using a master password** - If you do save passwords, set a Master password so they aren't easily accessible to anyone with access to the system. For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) > Privacy & Security > Browser Privacy section. Check "Use a master password". Set a master password that is compliant with campus [Password Standards](https://its.ucsc.edu/security/passwords.html#store) Note: The master password setting is not appropriate for passwords that provide access to [P3 or P4 sensitive data](https://its.ucsc.edu/policies/data-protect.html).



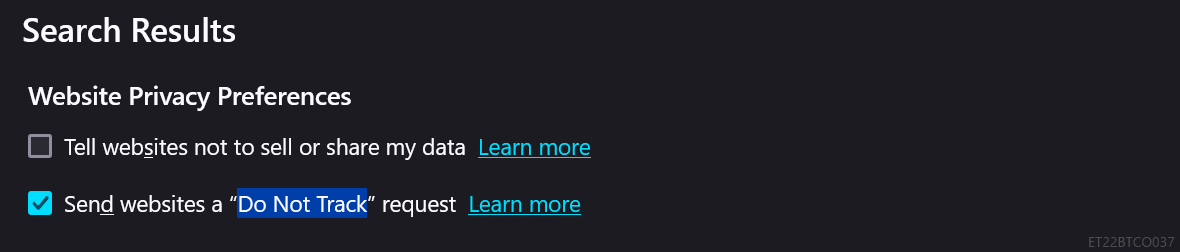
**Java/javascript** - Java is now disabled by default in Firefox, but can be activated for trusted sites.



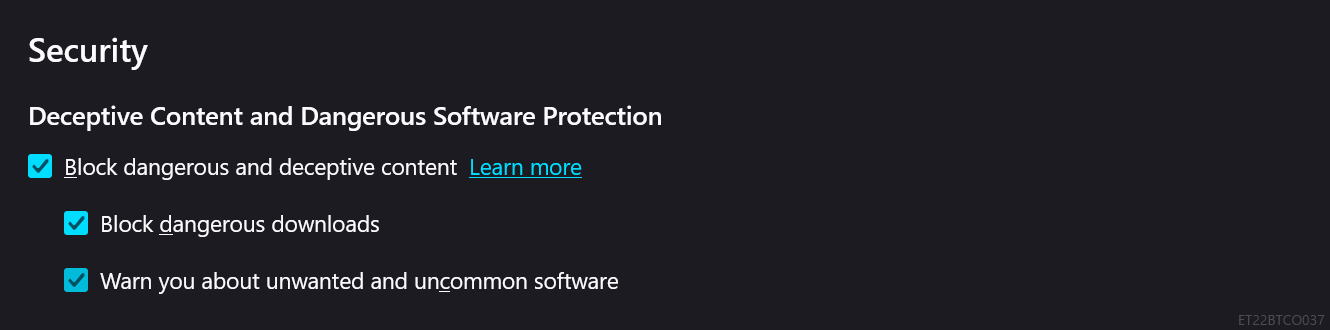
**Cookies and Site Data** - For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) > Privacy & Security > CContent Blocking. Select "Custom" and set Cookies to block "Third-party trackers". Also place checks to block Cryptominers and Fingerprinters.



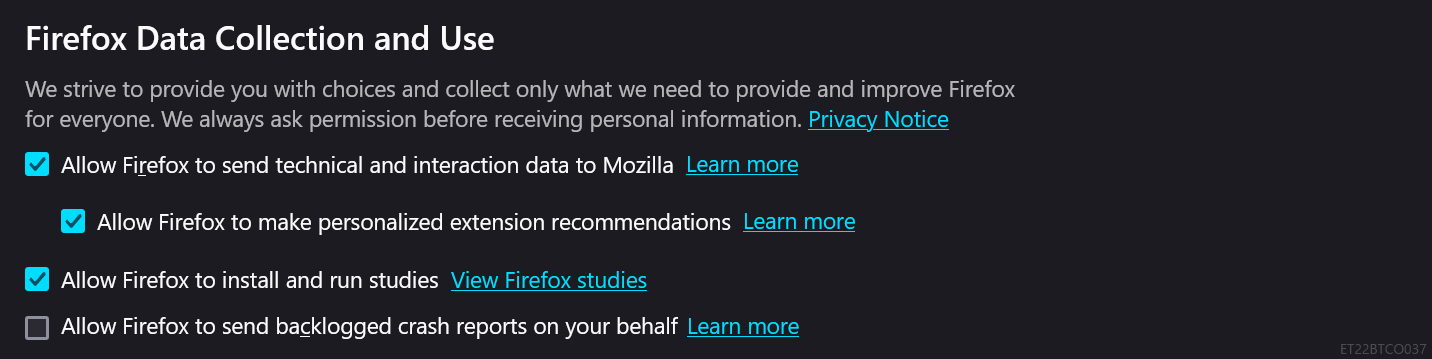
**Tracking Protection** - For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) > Privacy & Security > Content Blocking. Check "Always" under "Send websites a “Do Not Track” signal that you don’t want to be tracked".



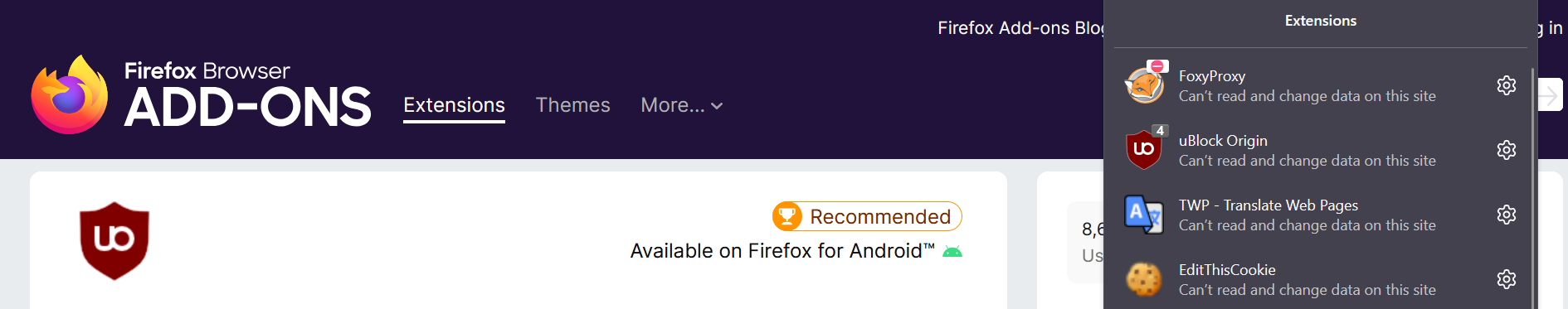
**Deceptive Content and Dangerous Software Protection** - For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) > Privacy & Security > Security section. Check "Block dangerous and deceptive content", "Block dangerous downloads" and "Warn you about unwanted and uncommon software".



**Firefox Data Collection and Use** - For both Mac and PC - go to Firefox menu > Preferences (Mac) Options (PC) > Privacy & Security > Firefox Data Collection and Use section. Uncheck "Allow Firefox to send technical and interaction data to Mozilla", "Allow Firefox to install and run studies" and "Allow Firefox to send backlogged crash reports on your behalf".



**Install uBlock Origin (Ad-blocker)** - Add-ons > “[uBlock Origin](https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/)” by Raymond Hill



**Conclusion:**

I learned how to secure a web browser by applying important safety measures to Mozilla Firefox. I implemented steps like enabling automatic updates, using strong passwords, and activating safe browsing features. I also added trusted security extensions and managed cookies and trackers. By following these actions, I successfully improved the browser’s security, ensuring better protection of personal data and privacy while browsing.