BROWSER SECURITY RESOURCES:

Here are some great links for websites to offer you more choices with respect to Browser Security. Please spend some time becoming familiar with them, and bookmarking them for future reference.

- https://www.wired.com/story/how-to-lock-down-websites-permissions-access-webcam/
    - Here is a great article that guides you through your privacy settings on each major browser

- https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm
- https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm
- https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/
    - uBlock Origin is a free and open-source, cross-platform browser extension for content-filtering, including ad-blocking. The extension is available for several browsers: Safari, Chrome, Edge, Firefox

- https://chrome.google.com/webstore/detail/disconnect/jeoacafpbcihiomhlakheieifhpjdfeo
    - **Disconnect**, which is a fantastic browser extension, similar to uBlock Origin that we discuss in the training, and that can be used on Chrome. I highly recommend it as well

- https://www.ghostery.com/
    - Ghostery has a great privacy-based browser similar to Brave, and helps you browse smarter by giving you control over ads and tracking technologies to speed up page loads, eliminate clutter, and protect your data. Its well worth checking out

- https://cliqz.com/en/
    - Cliqz is also another wonderful privacy-based browser similar to Brave and Ghostery, and worth checking out

- https://themarkup.org/blacklight
    - Type any website URL into this BlackLight tool, and it will tell you who all the trackers are that are running in the background, as well as what they are up to. Trust me, this tool will really make your blood boil!

- https://www.androidguys.com/tips-tools/how-to-disable-personalized-ads-on-android/
    - How to disable personalized ads on Android

- https://helpx.adobe.com/flash-player/kb/uninstall-flash-player-windows.html
    - How to disable Flash on a Windows system

- https://helpx.adobe.com/flash-player/kb/uninstall-flash-player-mac-os.html
    - How to disable Flash on a Mac
- https://computers.tutsplus.com/tutorials/how-to-uninstall-disable-and-remove-adobe-flash--cms-24414
    - Another helpful site showing how to disable/remove Flash

- https://www.howtogeek.com/222275/how-to-uninstall-and-disable-flash-in-every-web-browser/
    - This site also shows how to disable Flash from every browser

- https://chrome.google.com/webstore/detail/windows-defender-browser/bkbeeeffjjeopflfhgeknacdieedcoml
    - This plugin brings Microsoft Edge's phishing protection to Chrome as an extra defense-in-depth

- https://noscript.net/
    - The free NoScript Firefox extension provides extra protection for Firefox, and other mozilla-based browsers. It will allow **Java-**

Script, Java, Flash and other plugins to be executed only by **trusted web sites of your choice** (e.g. your online bank). As such, it will block any cryptomining scripts if you accidentally visit a site that has them running, and have scripts blocked by default

- https://blog.cloudflare.com/announcing-warp-plus/

- https://private-network.firefox.com/
  - Mozilla Private Network is brilliant! Its a simple, and free, browser extension that encrypts all the data leaving your browser (sort of like a browser-VPN if you will), and sends it over to **Cloudflare** (a trusted content delivery provider that promises to delete all your logs after 24 hours). This is great, as it bypasses your ISPs altogether, who have been known to sell your browsing data to 3rd party marketing firms.
  - On a similar note, you can also install Cloudflare's very own "**1.1.1.1 + Warp**" app, which will similarly keep your mobile phone's web traffic from being snooped by your ISP.
  - Both a great resources you should really consider: