**HTTP Filters, Ad and Track Blockers**

**The more extensions a browser has, the more unique it becomes and makes it easier for fingerprinting**

* Always install in a test environment or profile first

**uBlock Origin**

Voluntary development (no money involved – no censorship or motives)

HTTP firewall that blocks undesirable content based on certain rules

Light on CPU usage in its basic form

Dynamic filtering

The logger will show every request and blocks

Enable advanced mode

* Allows selections to block other things
* Uses more CPU

Prevent webRTC

* A possible way of getting real IP when using VPN or Tor etc

Can block:

* Images
* 3rd party trackers
* Inline scripts
* 1st party scripts
* 3rd party scripts
* 3rd party frames
* In general, or for specific sites

**uMatrix**

Made by same developers as uBlockO

User agent spoofing

* Pretend to be from a different browser or OS
* Referrer spoofing
  + Spoof the HTTP referrer so sites won’t know where you came from
* Strict HTTPS
  + Will use the HTTPS if available in preference to HTTP

However, all plugins store settings and preferences you make as well

**Disconnect.me**

* List of blocked sites
* Firefox has this built in anyway
* Can also add this list to things lie uBlock anyway

**RequestPolicy**

* uBlock uses filters to block however, this **blocks all cross-site requests** unless allowed
* main benefit is to prevent from cross-site tracking and cross-site request forgery attacks

**NoScript**

Allows active content to run only from sites that you trust

Protects from cross-site scripting attacks and clickjacking attacks

Lockdown what scripts can do and where

Integrated into back end of Tor browser

**VirusTotal**

* check sites for malware etc.

**Purify**

* ad blocker for iOS