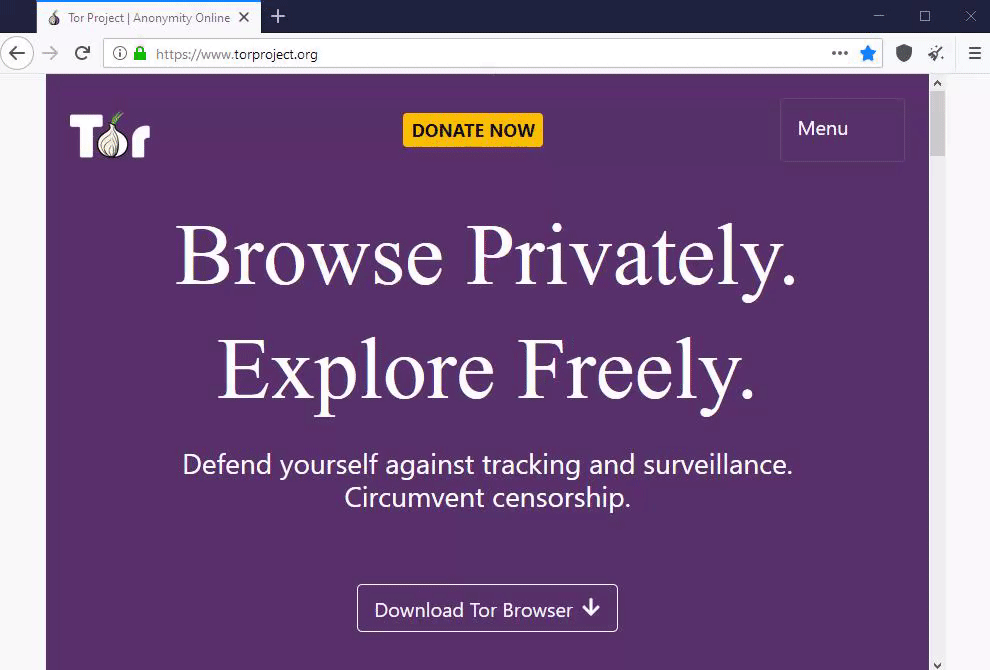
[SECURITY SETTINGS](https://tb-manual.torproject.org/security-settings/)

By default, Tor Browser protects your security by encrypting your browsing data. You can further increase your security by choosing to disable certain web features that can be used to attack your security and anonymity. You can do this by increasing Tor Browser's Security Levels in the shield menu. Increasing Tor Browser's security level will stop some web pages from functioning properly, so you should weigh your security needs against the degree of usability you require.

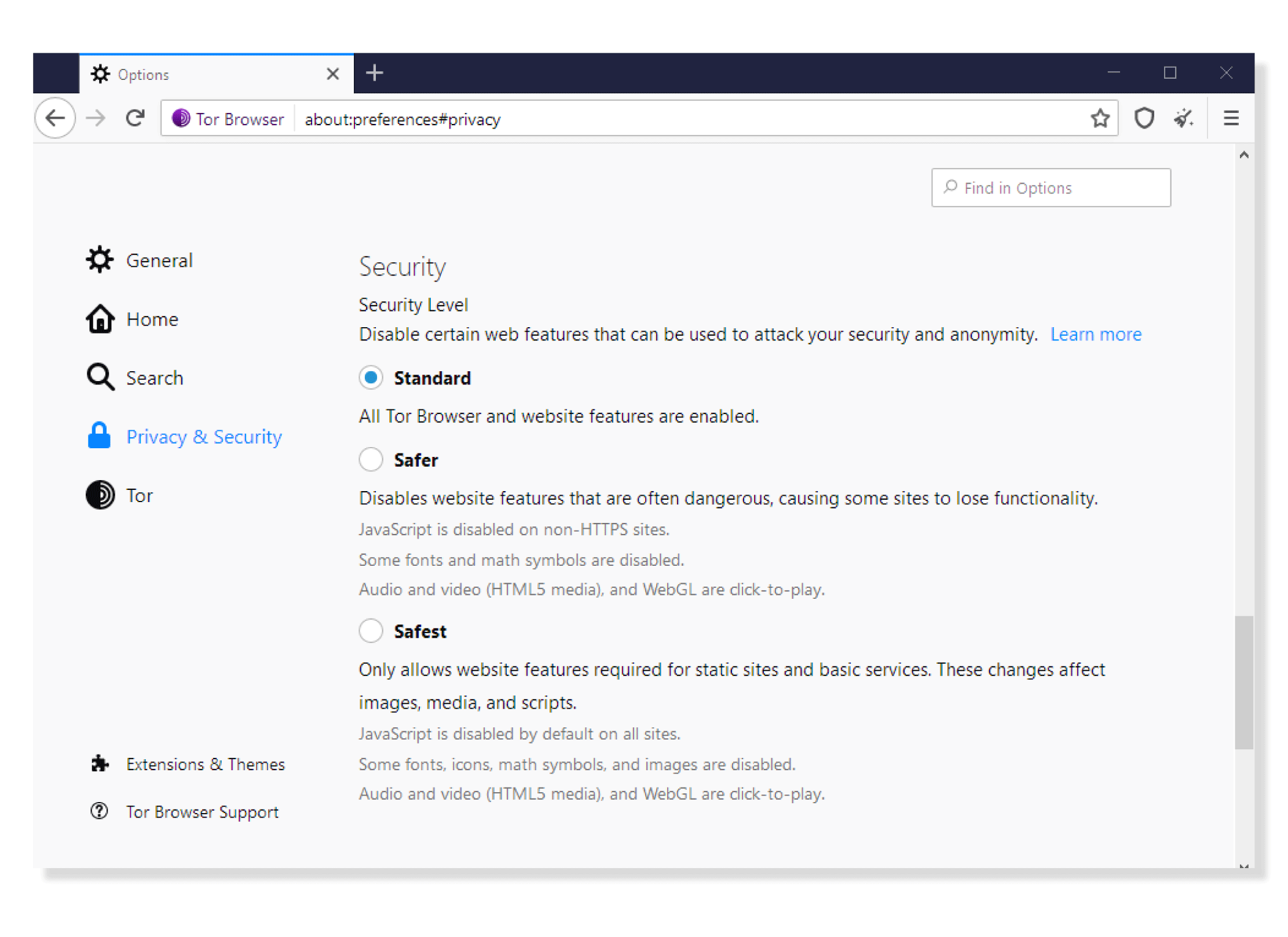
ACCESSING THE SECURITY SETTINGS

The Security Settings can be accessed by clicking the Shield icon next to the Tor Browser URL bar. To view and adjust your Security Settings, click the 'Advanced Security Settings...' button in the shield menu.



SECURITY LEVELS

Increasing the Security Level in the Tor Browser Security Settings will disable or partially disable certain browser features to protect against possible attacks. You can enable these settings again at any time by adjusting your Security Level.



**Standard**

* At this level, all Tor Browser and website features are enabled.

**Safer**

* This level disables website features that are often dangerous. This may cause some sites to lose functionality.
* JavaScript is disabled on all non-[HTTPS](https://tb-manual.torproject.org/secure-connections) sites; some fonts and math symbols are disabled; audio and video (HTML5 media) are click-to-play.

**Safest**

* This level only allows website features required for static sites and basic services. These changes affect images, media, and scripts.
* Javascript is disabled by default on all sites; some fonts, icons, math symbols, and images are disabled; audio and video (HTML5 media) are click-to-play.