CRYPTO PARTY

CRYPTOPARTYNEWCASTLE.ORG

Using the Tor Browser on Linux

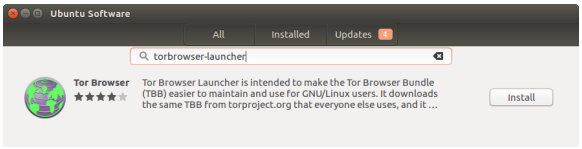
The Tor Browser is a customised version of the free-and-open-source Firefox web browser that makes it easy to protect your browsing activity by passing it through the Tor network.

Installation

The easiest method of installing the Tor Browser is probably using the **torbrowser-launcher** package, which is available in most popular distributions.

This package will handle downloading the Tor Browser for you, as well as verifying that the version downloaded has been legitimately produced by the Tor Project team.

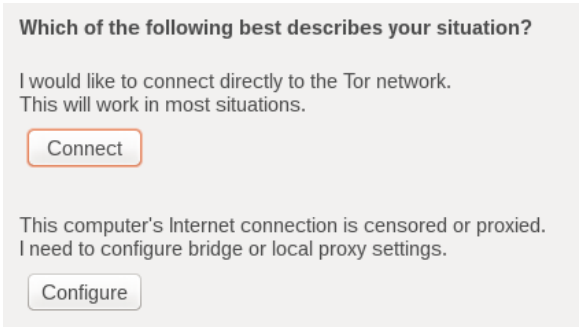
You can install this package using your favourite command-line tool, or ifnd it in the software centre by searching for the package name.



Once you have installed the package, you will have two new entries in your applications menu. Open the 'Tor Browser' entry to start the download and installation process for the Tor Browser.

First Launch

When you first launch the Tor Browser, you will see a prompt (below) asking you whether you wish to connect directly to the Tor network.

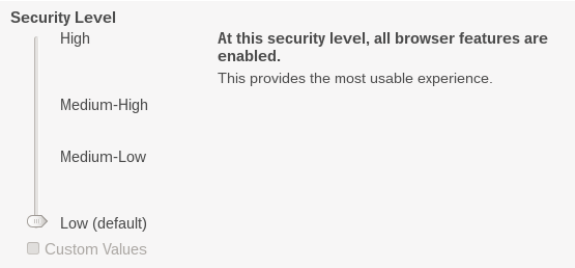


If you are connecting to Tor from a country with heavily censored internet access, please seek additional information and advice before choosing to directly connect to Tor at the above prompt.

However, in most cases, UK users will want to select the option to connect directly to the Tor network.

Settings

The Tor Browser features a security panel (which you can open from the Onion icon on your browser toolbar). This 'Onion Menu' has a slider allowing you to adjust the browser's security level.



Some features of a normal web browser may reveal your identity to a site, or make you vulnerable to attacks. Turning the security slider to a high setting disables some of these features, making you safer from well-funded attackers who can interfere with your internet connection, or use new unknown vulnerabilities in these features.

Unfortunately, turning off some of these features can lead to some websites that use them becoming unusable. The default 'Low' setting is fine for everday privacy protecion, but you can choose to set it to 'High' if you are worried about sophisticated attackers, or if you don't mind that some websites may display incorrectly.

Browser Add-ons

For security purposes, the Tor Project team recommend you do not install additional Add-ons into the Tor Browser, as they may interfere with how Tor works and cause the browser to leak your identity to the sites you visit.

Usage

That's it! You can now use the Tor Browser as you would use a normal web browser, and browse the internet while protecting your privacy and anonymity.

You may wish to read the Tor Project website for more detailed information on staying secure.

Please visit `torproject.org` for more information.