How to use Tor Browser to surf anonymously

The purposes for using Tor are to distribute incoming and outgoing traffic through a series of virtual tunnels, possibly from reporters to keep private confidential messages to everyday internet users who want to access Websites are restricted by the service provider. In fact, some people choose to exploit Tor for nefarious purposes, but most web surfers just want to prevent websites from tracking every action or determining their geographic location.

With the increasingly tight supervision of employers, schools and even governments, anonymity while browsing the web has become a top priority for many users. Users of particular interest in privacy are switching to Tor (The Onion Router), a network originally created by the US Navy and now widely used globally.

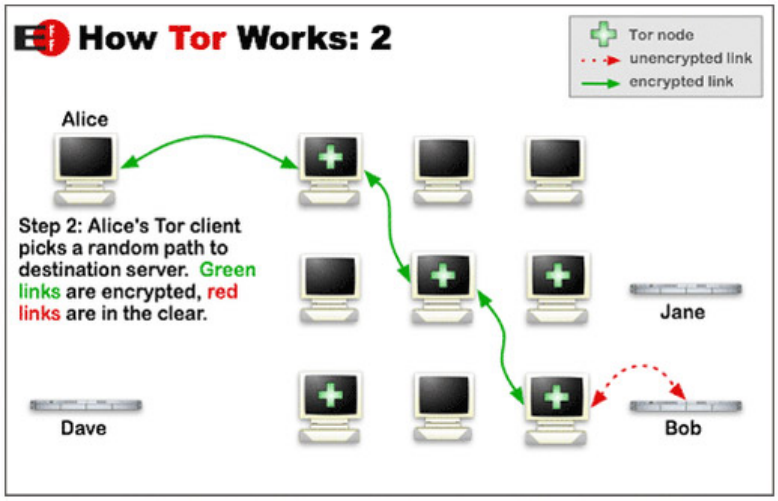
The purposes for using Tor are to distribute incoming and outgoing traffic through a series of virtual tunnels, possibly from reporters to keep private confidential messages to everyday internet users who want to access Websites are restricted by the service provider. In fact, some people choose to exploit Tor for nefarious purposes, but most current web surfers just want to prevent websites from tracking every action or locating their geography.

Connect to the Tor network with the Tor Browser from the computer quite quickly and safely. Find out how to use the Tor Browser to surf the web anonymously through the following article!

What is Tor?

Tor is a computer network operated by volunteers around the world. Each volunteer runs a relay - a computer running software that allows users to connect to the Internet via the Tor network.

Before accessing the Internet, the Tor Browser will connect to many different relay, wipe its routes in each step, making it hard to find out who you really are and where it comes from.



Tor is a good tool to keep the user's browser private with ISPs and advertisers.

Start with Tor

The easiest way to use Tor is to download the Tor Browser. This is a modified version of Firefox along with a host of other software that connects users to the Tor network.

Tor Browser Bundle is available for download on countless websites. However, we recommend that you only download the Tor Browser from torproject.org, Tor's official homepage. Users can choose from more than a dozen languages, from English to Vietnamese.

To start the download process, navigate to your current browser to **https://www.torproject.org/projects/torbrowser.html.en** . Next, scroll down until you find your desired option in the **Language** column, click the link found below the title corresponding to your specific operating system. When the download is complete, find the Tor file and launch it. Mac users double click on the downloaded file to open the **.dmg** image. After opening, drag the Tor file displayed in the **Applications** folder. Linux users should use the proper syntax to extract the downloaded package and then launch the Tor Browser

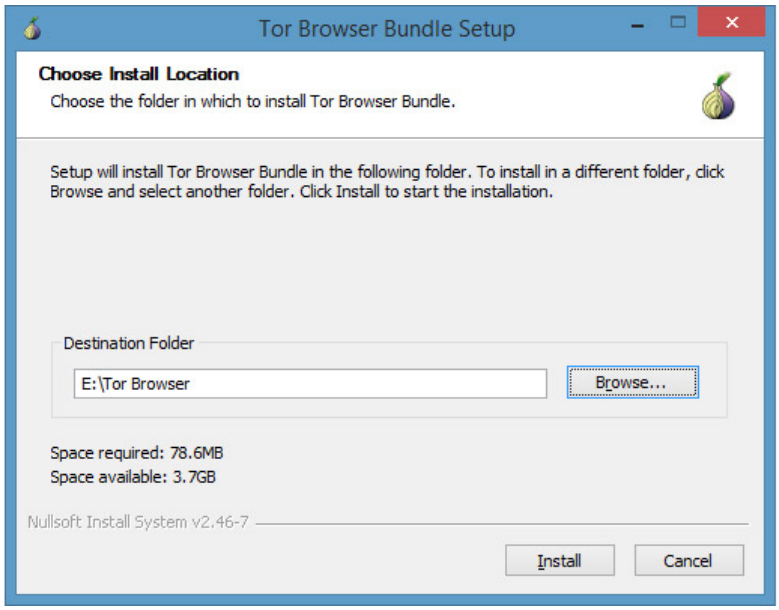
file.

Once you have downloaded the installer, you have two options: Install the software or check the GPG signature of the previous installation file. Some people want to check the installation file to make sure they have downloaded the appropriate browser version and not something that is fake.

But GPG signature checking is not an easy process and it requires downloading additional software.

Install Tor

Whether or not you have checked the GPG signature, the next step is to install the Tor browser.



For Windows, the Tor Browser appears as an **EXE** file, so it's basically like installing any other program. The main difference is that the browser does not have the same default location as most other programs. Instead, it selects the **desktop** as the installation location.

The Tor Browser does this because it is portable and does not integrate into the Windows system the way regular programs do. This means that you can run the Tor Browser from virtually anywhere - Desktop, document folder or even a USB drive.

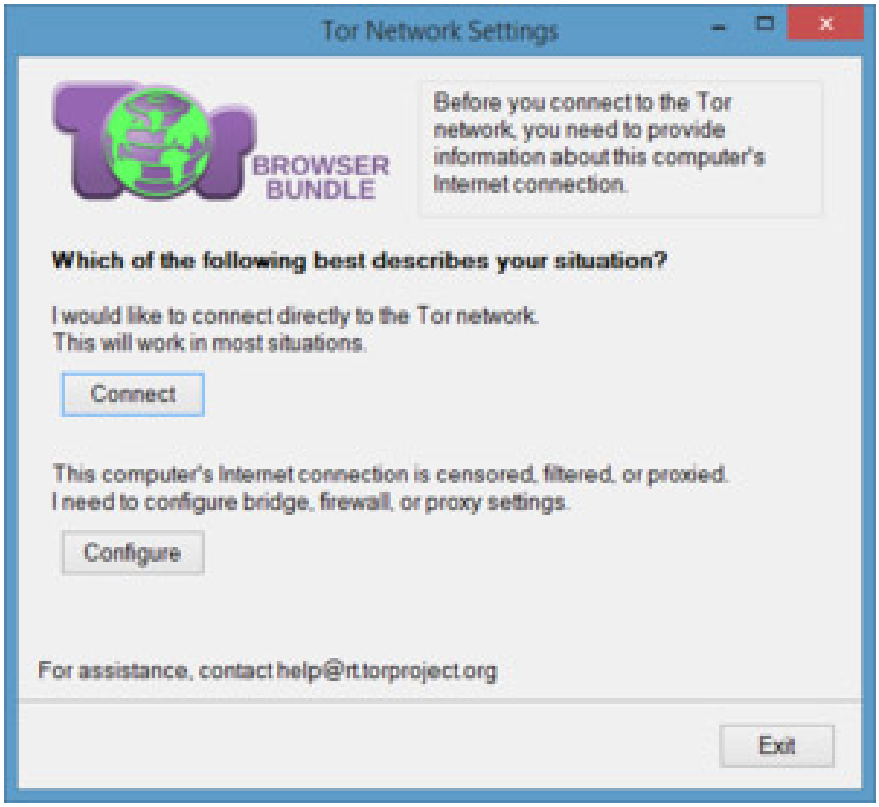
When you go to the **Choose install location** window, click **Browse .** and then choose where you want to install the browser. As you can see in the image above, we installed it on a USB drive.

Once you've selected your location, simply click **Install** and Tor will handle the rest.

Use the Tor Browser

When the browser is installed, you will have a folder called Tor Browser. Open it and inside you will see " **Start Tor Browser.exe** ". Click on that file and a new window will open asking if you want to connect directly to the Tor network or if you need to configure proxy settings first.

Most people choose to connect directly to the Tor network to get started. Choosing the live option is best for almost all users, so choose **Connect** . A few seconds later, a version of Firefox will start. You are then connected to the Tor network and can browse the web anonymously.



To ensure you are connected to Tor, visit **whatismyip.com** . This feature will automatically detect your location based on your IP address. If the browser shows you are from a place other than your current location, everything is working well. Make sure you perform all of your anonymous browsing activities from the Tor Browser because other programs on the system are not connected to Tor.

However, anonymous browsing on Tor is not as easy as starting the program. There are a number of rules you should observe, such as connecting to every site through SSL / TSL (HTTPS) encryption. If you do not do so, anything you do online can be observed by another person. This browser has an HTTPS Everywhere add-on of the Electronic Frontier Foundation installed by default, ensuring most of your SSL / TSL needs.

Connect with Tor

As soon as the browser is launched, the connection to the Tor Network will be initialized, depending on the user's own settings. Please be patient, as this process may take a few minutes to complete.

When the connection to Tor is set, the **Status** screen will disappear and the Tor Browser itself will start after a few seconds.

Browse the web via Tor

The Tor browser will now display in the foreground. All incoming and outgoing traffic generated through this browser will be routed through Tor, providing a relatively safe and anonymous browsing experience. When started, the Tor Browser application will automatically open a Web site hosted on **torproject.org** , which has a link to check your network settings. Selecting this link will display your current IP address on the Tor network. Since you are in incognito mode, you will notice that this is not a real IP address.

If you want to see this content in another language, use the drop-down menu found at the top of the page.

Torbutton

In addition to many standard Firefox features, such as bookmarking and source analysis through an integrated Web development toolkit, the Tor Browser also includes many unique functions. One of these components is Torbutton, found in the browser address bar.

Torbutton allows you to modify specific proxy and security settings. Most importantly, it offers the option to switch to a new identity - ie switch to a new IP address - with a simple click. Torbutton options, described below, are accessible via the drop-down menu.

1. **New Identity** : Specify a new random IP address for the active Tor connection. To select this option, users will be asked to restart the browser to activate.
2. **New Tor Circuit for this Site** : Instead of restarting the browser and setting up a completely new identity, this option will immediately create a new circuit for the active tab.
3. **Privacy and Security Settings** : Open the dialog box with configurable settings including private browsing mode settings, third-party cookie behavior, prevent Flash and other plugins from running, etc. This feature also allows You specify Tor's security level through a slider, from low to high.
4. **Tor Network Settings** : Allows you to configure proxy settings and firewalls as well as specific settings for ISPs. Also contains a button that copies the contents of Tor's log file to the clipboard.
5. **Check for Tor Browser Update** : Make sure you are running the latest Tor Browser version.

NoScript

Tor Browser also has an integrated version of the popular NoScript utility. Accessible from a button on the Tor Browser main toolbar, this custom utility can be used to block all scripts running in the browser or just scripts on specific websites. The recommended installation is **Forbid Scripts Globally** .

HTTPS Everywhere

Another popular extension integrated with Tor Browser is HTTPS Everywhere, developed by the Electronic Frontier Foundation, ensuring that your communication with many leading websites is strongly encrypted. HTTPS Everywhere's functionality can be modified or disabled (not recommended) via the drop-down menu, accessible by clicking on the main menu button (located in the upper right corner of the browser window).).

Also, remember that anonymous browsing doesn't make you immune to viruses and other malware. Tor cannot protect you from malicious software used to steal information about your current location.

However, for regular Internet users, Tor Browser is sufficient to maintain online privacy.

See more:

1. Guide to anonymous web on Android phones
2. A guide to the Deep Web for newbies
3. How to switch open tabs in Firefox to private mode

You finished reading the article "**How to use Tor Browser to surf anonymously**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
