**[Access the Dark Web While Staying Anonymous with Tor](https://null-byte.wonderhowto.com/how-to/access-dark-web-while-staying-anonymous-with-tor-0179341/)**

* By [**Black Slash**](https://creator.wonderhowto.com/blackslash/)
* 10/23/2017 11:27 pm
* [Tor](https://null-byte.wonderhowto.com/how-to/tor/)

The dark web is an intimidating place for a newbie hacker, but it's a powerful tool once you've learned to navigate it safely. To help you out with that, this guide will cover some need-to-know information for traversing the dark corners of the internet while keeping your identity and data safe. (Hint: Using [Tor](https://null-byte.wonderhowto.com/how-to/tor/) is not enough.)

**The Wonders of the Dark Web**

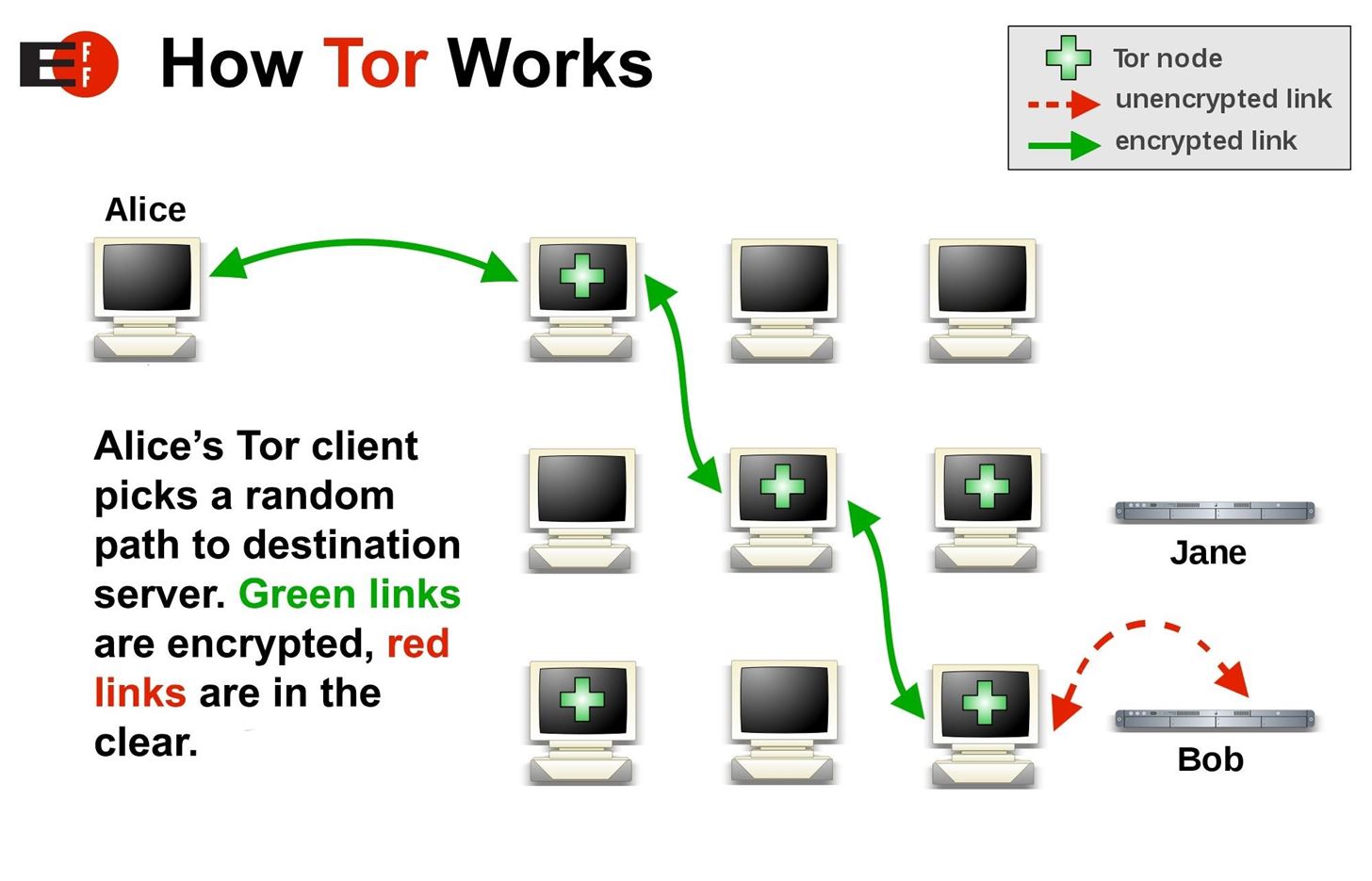
First off, we should establish that the term "dark web" refers to overlay networks running on top of the normal internet infrastructure, which need special permission or custom software to access. Three of the most popular dark web networks are I2P, Freenet, and Tor. For the purposes of this tutorial, we will talk about the most popular and widely known network, Tor.

Tor's intended purpose is to protect user's privacy through anonymity. It often gets a bad reputation for being used for criminal activity, such as buying and selling narcotics from sites like [the infamous Silk Road](https://null-byte.wonderhowto.com/how-to/with-silk-road-bust-online-black-market-already-has-new-home-0148878/) or [the recently shut-down AlphaBay](http://www.bbc.com/news/technology-40670010).

**Don't Miss:** [**How to Keep Your Internet Traffic Private from Anyone**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-keep-your-internet-traffic-private-from-anyone-0160987/)

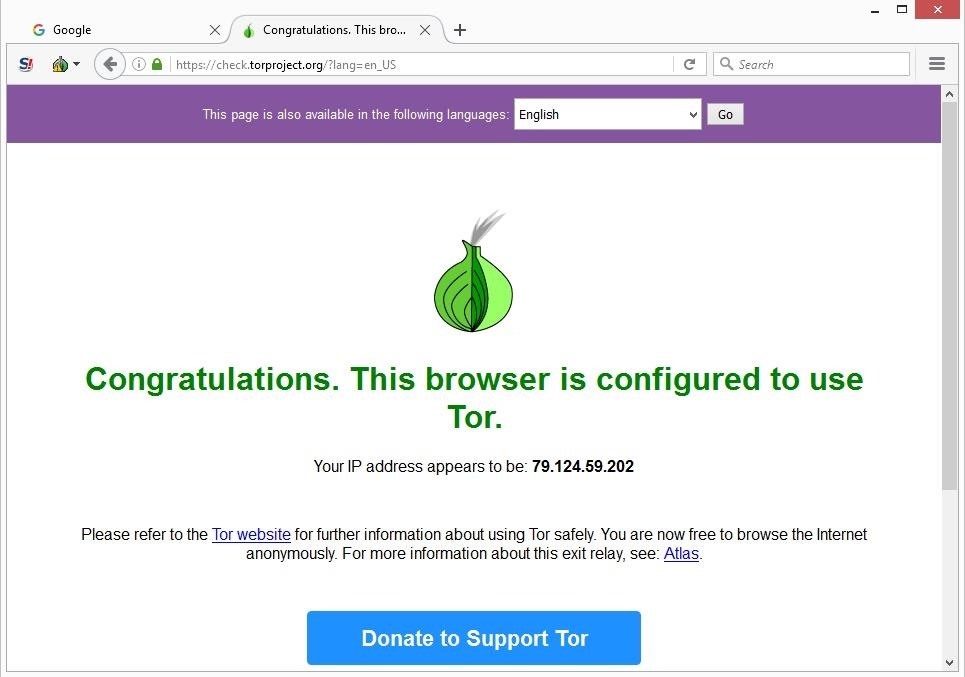
In spite of this, Tor has a much more noble history, often used by whistleblowers to expose government corruption or by regular people to circumvent oppressive government censorship [in places like Uganda](https://www.dailydot.com/layer8/uganda-censorship-circumvention-how-to/) or, rather famously, China. The United States Justice Department recently [even endorsed Tor](https://motherboard.vice.com/en_us/article/xyg45n/department-of-justice-official-tells-hundred-federal-judges-to-use-tor) for use by federal judges to keep their personal data private while working on controversial cases.

Tor, known as "[The Onion Router](https://null-byte.wonderhowto.com/how-to/tor-vs-i2p-great-onion-debate-0133642/)" due to its layered nature, is a network that runs on top of the regular internet and directs your web traffic through a series of relays before sending it to its final destination. If I were a journalist trying to expose government corruption in Uganda worried about censorship or surveillance, I would need to connect to services without my internet service provider knowing what I was really doing. If I wanted to reach a mail server through Tor, my request would travel encrypted along with a random path through the Tor network, rather than directly through my ISP.

[](https://img.wonderhowto.com/img/original/47/03/63639859057218/0/636398590572184703.jpg)

A description of how the Tor network functions. *Image via* [*Electronic Frontier Foundation*](https://commons.wikimedia.org/wiki/File:Tor-onion-network.png)

Each step along the way is encrypted, and my traffic might go to Tor nodes in France, and then Denmark, before finally reaching a final exit destination in the United States. While in transit, the Tor node can only see the IP address of the next location. By the time my request to access the mail server has reached the exit node in the United States, my original IP address is completely unknown, and in Uganda, my ISP would only see the encrypted traffic.

[](https://img.wonderhowto.com/img/original/76/75/63638760532376/0/636387605323767675.jpg)

Tor showing me what my IP address appears to be to the rest of the Internet. In this case, it’s in France.

**Installing & Using Tor**

There are several ways of accessing the Tor network, but for this tutorial, we are going to use the Tor Browser. The Tor Browser bundle is a good way for beginners to use Tor since it comes preconfigured in a way that is designed to maximize your privacy and security.

**Step 1Download the Tor Browser**

Downloading the Tor Browser is as simple as going to the [Tor Project website](https://www.torproject.org/projects/torbrowser.html.en#downloads) and selecting the appropriate file to download. Select your operating system, your language, and either the 32-bit or 64-bit version. If you're unsure, choose the 32-bit version.

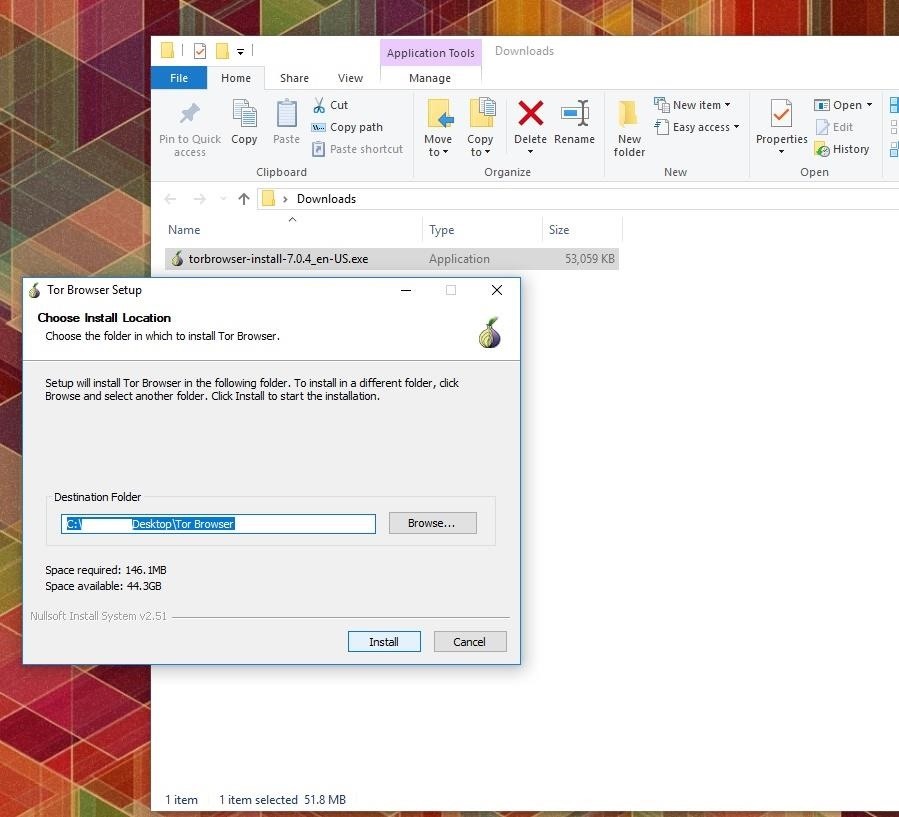
[](https://img.wonderhowto.com/img/original/44/40/63638879799508/0/636388797995084440.jpg)

**Step 2Install the Tor Browser**

The installation process for the Tor Browser is pretty basic but will vary slightly depending on your operating system. We've broken it down as follows. If you get stuck, additional instructions can also be found at the Tor Project website link above.

**Windows**

To install Tor on Windows, double-click on the Tor Browser install executable file. When prompted, enter your desired language and click "OK," then click "Install."

[](https://img.wonderhowto.com/img/original/65/19/63639622049259/0/636396220492596519.jpg)

**Linux**

Installing Tor on a Linux distribution can be done through the terminal. First, move to the directory where you downloaded the file by typing:

cd \_folder/subfolder/etc

Then unpack the .tar.xz file by typing:

tar -xvJf tor-browser-linux32-7.0.4\_en-US.tar.xz

In this command, the 32 will be replaced with 64 if you use the 64-bit version, the 7.0.4 refers to version, and en-US is for the English version.

Next, move to the directory you just created:

cd tor-browser\_en-US

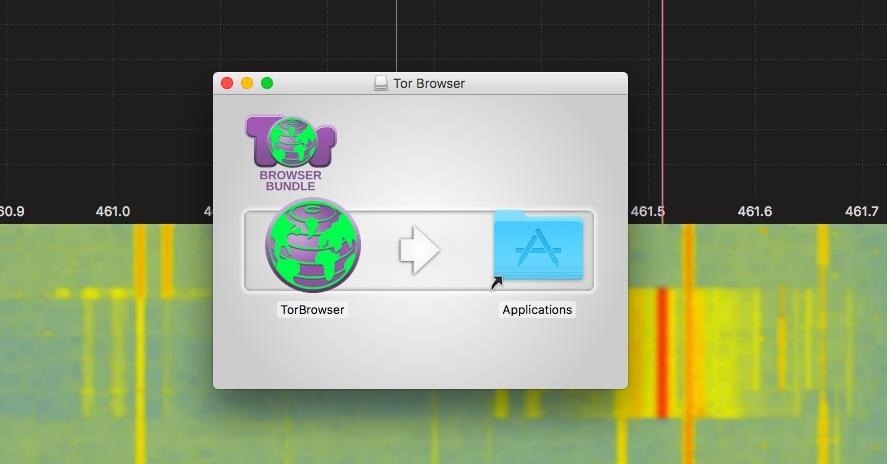
And then you can run the Tor Browser by typing the following (do not do this under the root user):

./start-tor-browser.desktop

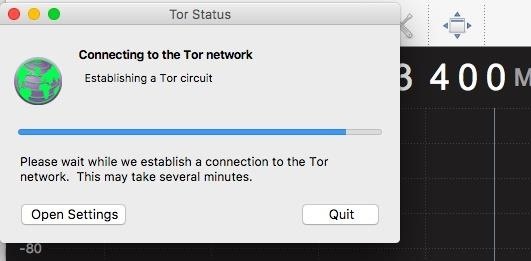
Alternatively, you can also click on the Tor Browser Setup icon in the file.

**macOS (Mac OS X)**

After downloading the file, click on it to open the .dmg file. Drag the Tor Browser app inside your applications folder, and open it.

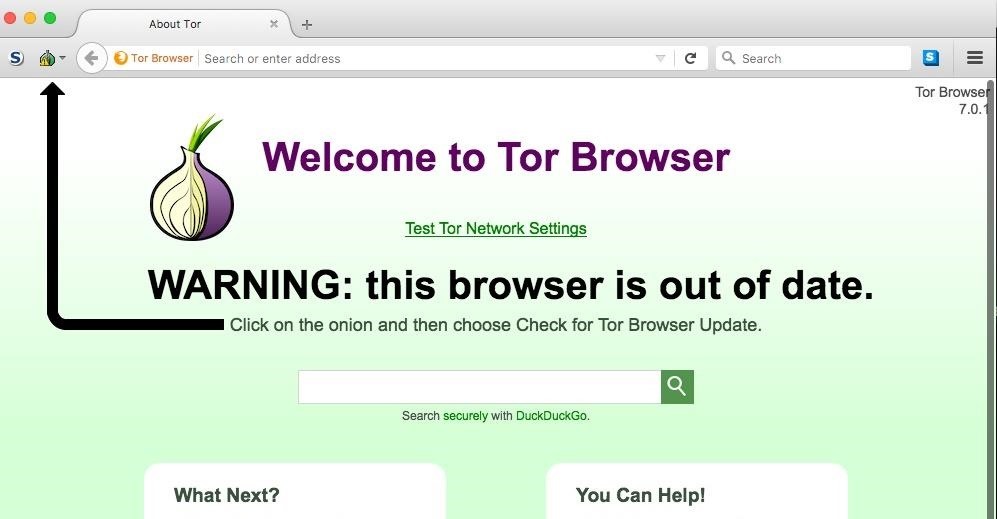
[](https://img.wonderhowto.com/img/original/55/31/63639660622120/0/636396606221205531.jpg)

After Tor builds a relay, a browser window will open. You're now connected to Tor, but make sure to update the browser if needed.

[](https://img.wonderhowto.com/img/original/25/65/63639660673841/0/636396606738412565.jpg)

Tor building a circuit.

The landing page will let you know if you need to update it before using the Tor Browser.

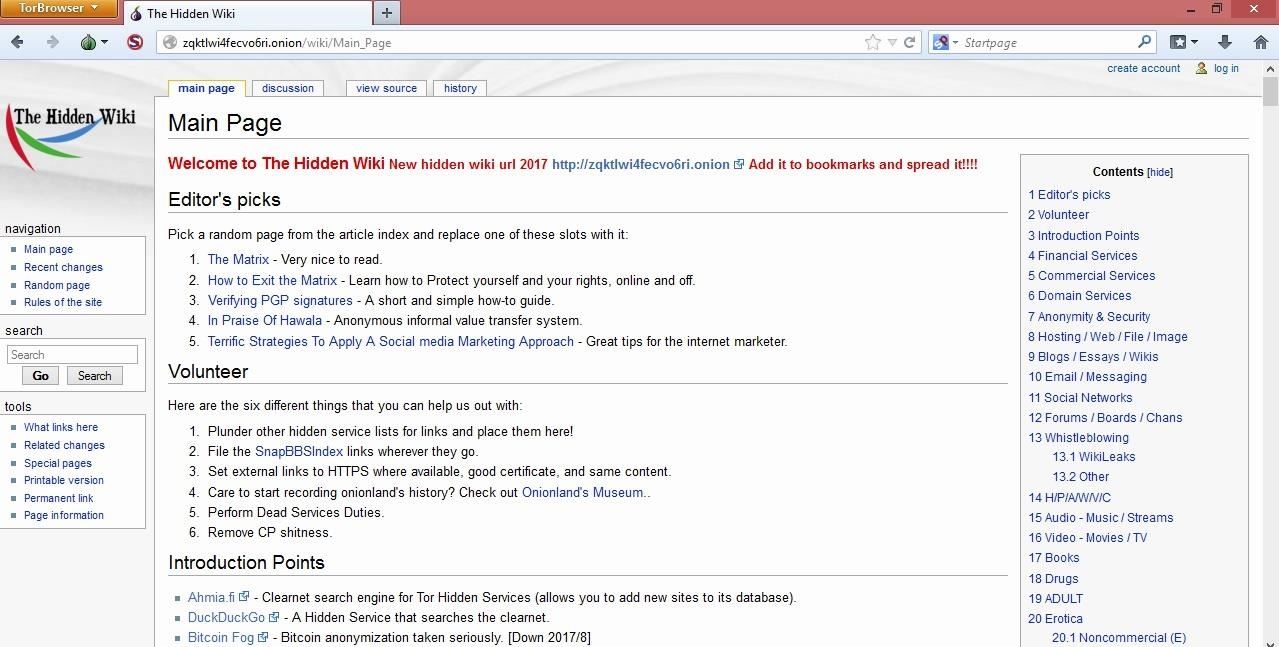
[](https://img.wonderhowto.com/img/original/91/67/63639660718934/0/636396607189349167.jpg)

Make sure to update!

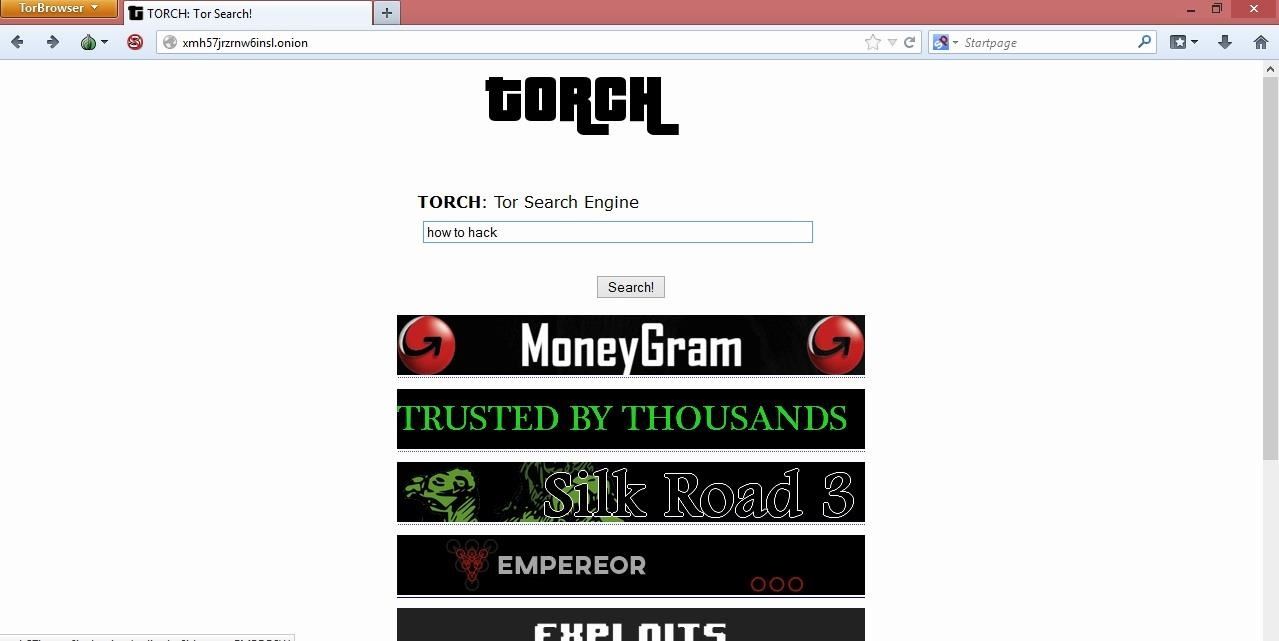
**Step 3Get Around on the Tor Network**

Accessing sites on the Tor network is not always straightforward. To navigate to regular internet websites, you can simply type a URL like [wikipedia.com](http://www.wikipedia.com) in the address bar. Sites that are hosted on the Tor network have an .onion domain, preceded by arbitrary characters. For example, *zqktlwi4fecvo6ri.onion* is the current location of the *Hidden Wiki*.

The Hidden Wiki is a good place to start when you're first familiarizing yourself with what Tor has to offer. It breaks down some of the most popular destinations on the network into categories and also has some interesting articles, like how to verify PGP signatures.

[](https://img.wonderhowto.com/img/original/03/69/63638880017149/0/636388800171490369.jpg)

In order to find sites on the Tor network, Google isn't going to be very helpful. There are several dark web search engines, the most popular one being Torch, but these are not going to get you everywhere you might want to go. Keep in mind that most of the Tor network is not indexed, and as such, you will need to know the exact URL of the website you wish to connect to in order to access it. Reddit or other communities can sometimes be helpful for this purpose.

[](https://img.wonderhowto.com/img/original/05/23/63638880274149/0/636388802741490523.jpg)

Torch, a Tor network search engine.

**Step 4Stay Anonymous on Tor**

Now that you know the basics of browsing the Tor network, it's time for more important tasks — keeping yourself anonymous. Tor alone is not enough to mask your identity.

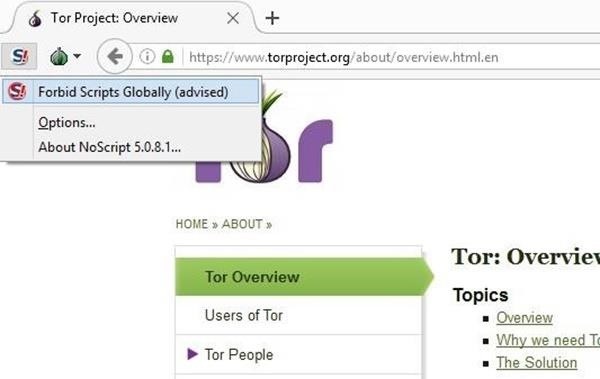
**Protect Your Identity**

In order to protect your privacy and stay anonymous when interacting on the dark web, you must assume a new identity. Never associate this new identity with details about the real you. This goes beyond making sure to never reuse old usernames — your anonymous identity should appear to be a completely different person than the real you. Leave all your real-world preferences, characteristics, and information behind if you want to stay anonymous.

**Disable Scripts**

The wonders of Flash and JavaScript make the internet very convenient nowadays. JavaScript is the reason Google can suggest search results in real time while you're typing because it's able to see your keystrokes, one by one. This is just one of the various ways that scripts can collect more information from users that could potentially compromise your security. In addition, scripts can be used in delivering malware, which can then expose your privacy and reveal details like your real IP address.

For these reasons, you'll want to disable scripts in the Tor Browser to prevent websites from obtaining identity compromising information. Do this by selecting the "S" icon in the top-left corner of the Tor Browser window.

[](https://img.wonderhowto.com/img/original/55/97/63639863861117/0/636398638611175597.jpg)

Disabling scripts on the Tor browser.

**Use Encryption When Communicating**

To stay anonymous when you're communicating on the Tor network, it's a good idea to use encryption. Many of you may be familiar with PGP encryption, or have at least seen something that looks like this:

[](https://img.wonderhowto.com/img/original/94/07/63638880714492/0/636388807144929407.jpg)

This is a PGP public key, something you're going to see often on your [deep web](https://null-byte.wonderhowto.com/news/anonymity-darknets-and-staying-out-federal-custody-part-one-deep-web-0133455/) exploits. You're going to need this in order to encrypt messages intended for the owner of that key. To make life more convenient, there are several tools available that allow you to quickly encrypt and decrypt messages in PGP such as [Kleopatra](https://www.kde.org/applications/utilities/kleopatra/). For more information on PGP encryption, check out one of our tutorials about it:

**More Info:** [How to Use GPG4Win in Windows to Encrypt Files & Emails](https://null-byte.wonderhowto.com/how-to/use-gpg4win-windows-encrypt-files-emails-0148943/)

Whether you use PGP or a more advanced encryption method, having your communication encrypted is essential to maintaining anonymity, especially if you're using it to communicate private information like an address, for example.

**Don't Download Anything**

Downloading files from the Tor network is a big no-no. First, it wastes network resources which are unequipped to deal with that kind of traffic. Secondly, files you download to your computer could easily contain malware which sends back your real IP address or exposes your identity in other ways. If you must download something off the Tor network, make sure it is from a source you trust.

**Step 5Things to Be Mindful Of**

While we've already discussed anonymity above, there are a few more things you need to consider when browsing the Tor network with the Tor Browser.

**Tor Exit Nodes**

One of the major risks of Tor is using exit nodes. When your traffic is routed through the Tor network, the last jump from a Tor node to your destination is not encrypted. Because Tor exit nodes are notoriously used for criminal behavior, some services will detect and blacklist activity originating from a Tor exit node. If you connect to most IRC chat rooms through Tor, for instance, IRC will only see that the IP address connecting to it is an address on a Tor network exit node, and you will be K-lined (IP banned).

In general, be mindful of the fact that just because you are using Tor to stay anonymous, any place you go to can still see that you are using Tor.

**Beware of Bitcoins**

Bitcoin is often purported as an anonymous currency, but this somewhat misleading. While there is no hard link between your real identity and your bitcoin activity, there are two crucial things to keep in mind.

The first is that your bitcoin address and all of its history will be available to anyone because of the nature of the blockchain — a database that records every bitcoin transaction in history. The second issue is that any reputable bitcoin wallet service will require an authentication of your identity in order to exchange bitcoins for real world currency. While this information is kept only in the hands of the exchange service, it does pose a threat as a tangible link between your real-world identity and your deep web presence.

[](https://img.wonderhowto.com/img/original/29/25/63639661805738/0/636396618057382925.jpg)

Bitcoin is often associated with the Tor network. *Image by BTC Keychain/*[*Flickr*](https://www.flickr.com/photos/btckeychain/9714198380/)

**Don't Miss:** [**The Best Bitcoin Wallet Apps for Your Android Device**](https://android.gadgethacks.com/how-to/best-bitcoin-wallet-apps-for-your-android-device-0176409/)

If you want to take an extra step to make sure your bitcoins can't be traced back to your unique wallet address, you can use a bitcoin mixer, sometimes also called a bitcoin tumbler. Some examples include [Shadow Wallet](https://shadowrnzghb5zhb.onion.link/) and [EasyCoin](https://easycoinsayj7p5l.onion.to/). Mixer services act as a middle man between your bitcoin address and the address you're sending them to. Everyone that is using that services has all their bitcoins put a giant pool and mixed around before they are sent. This way, the bitcoins that reach the recipient are from a variety of different address unassociated with yours.

**Timing Attacks**

Timing and correlation attacks can be used to pinpoint someone's IP address by comparing the timing of outgoing traffic to traffic that appears on the other end of the Tor network. While this requires a lot of patience and resources, It can ultimately be used to reveal your identity. This tactic is generally reserved for government agencies like the FBI and NSA to catch high profile targets like terrorists or large-scale narcotics distributors. You can read more about timing attacks on [DeepDotWeb](https://www.deepdotweb.com/2016/10/25/tors-biggest-threat-correlation-attack/).

**Tor Is Always Risky**

This tutorial is a good starting point to help you protect your privacy on the dark web. It is by no means a comprehensive list of everything that could be done to preserve your anonymity. No matter how hard you try to conceal your real identity when using Tor, there is always a risk, however small, that you will be discovered. Keep this in your mind when making decisions about what you do on the dark web.

Hopefully, you've gained some basic knowledge you can use to arm yourself for your new dark web exploits. Good luck, be careful, and don't be a terrorist!