

How to Become Anonymous on the Internet Using Tor

By [Alex Long](#) 10/08/2011 1:56 am

The internet is a scary place, and if you're like me, you don't want anyone tracking you or learning your search habits. It's a blatant invasion of privacy for companies to do this, but at least we have methods of fighting back—one of which is [Tor](#).

Tor stands for **The Onion Router**. It operates by donated bandwidth from its users. Tor encrypts your traffic, then forwards it through multiple nodes, like the layers of an onion, hence the name "The Onion Router". It protects you by masking your IP (Internet Protocol) address, which is synonymous to your home address. It also protects you by tunneling all of your traffic automatically, as if you had [set up a VPN](#), or [SSH tunnel](#). Most of the time, [Google Sharing](#), a Firefox plugin by [Moxie Marlinspike](#), will suffice. But sometimes I need to be fully anonymous.

Now, be forewarned, Tor isn't fully anonymous. Some things are left to the user to fix, such as changing your User Agent. A User Agent reveals your OS (operating system) and browser information. I'm a privacy nut, so I don't like people having that either. Also, you probably shouldn't be logging onto Facebook, as that will obviously reveal your information.

In this [Null Byte](#), we're going to go briefly go over how to set up Tor, after which I will forward my traffic through it to show you that it's working. The methodology is the same on Windows and Linux, but I'll use Windows to avoid confusion.

Download & Configure Tor

Follow along with the video and the instructions below.

1. Download [Tor](#).
2. Install Tor.
3. Navigate to the Data/Vidalia folder, and comment out the Browser line with "#" prefacing it.
4. Run Tor.
5. Download [Torbutton](#).
6. Restart Firefox and click the Torbutton, and it will run using Tor.