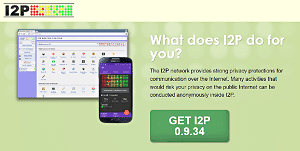
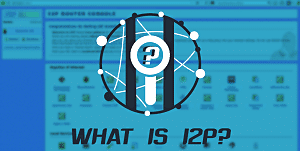
n the following article, we are going to provide you witha step by step I2P guide that is simple to follow and free of techie jargon.

We are also going to map out I2P and its alternatives, taking a look at their strengths, weaknesses, and differences in detail.

If you already know what I2P is, then go ahead and jump straight to our step-by-step [how to use I2P section.](https://proprivacy.com/privacy-service/guides/i2p-guide#how-to-use-i2p)

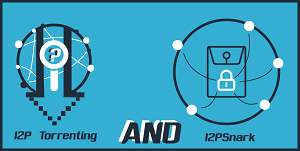
**What is I2P?**



The Invisible Internet Project (I2P) is a decentralized anonymizing network built using [Java](https://en.wikipedia.org/wiki/Java_%28programming_language%29) on similar principles to Tor, but which was designed from the ground up as a self-contained darknet.

I2P is effectively an internet within an internet. Once connected you can send email, browse websites, use blogging and forum software, host websites, take advantage of decentralized file storage, engage in anonymous real-time chat, and much more. As noted, you can also surf the open web anonymously, but I2P is probably not the best tool for the job in this regard.

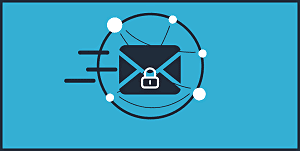
**I2P Torrenting and I2PSnark**

Most of the time anonymizing networks serve as an effective tool for torrenting copyrighted data. Torrenting is very popular, but it’s risky it is not anonymous, and that’s where networks like VPN and I2P come in handy.

I2P torrenting is becoming increasingly popular, and there is a torrent client exclusively designed for I2P. [I2PSnark](https://www.klomp.org/snark/) is basically a torrent client for the I2P network that uses the BitTorrent protocol. It is also a torrent creator that delivers metainfo.torrent files equipped with an in-built tracker.

We also must note that ProPrivacy certainly does not encourage this. If you want more information about staying secure, check out our [best VPN for torrenting](https://proprivacy.com/vpn/comparison/best-vpn-torrenting) guide.

**I2P Bote**

****

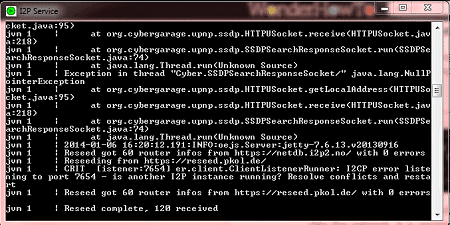
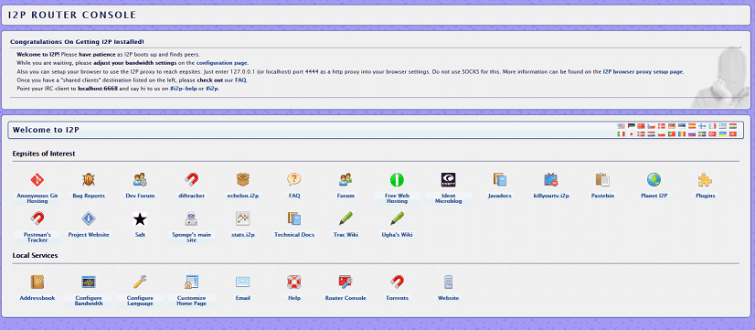
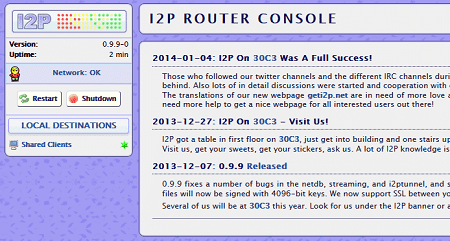
I2P has two main messaging services, one of them is I2P Bote. It’s a service for secure and anonymous messaging, therefore you are not able to send messages for the “visible” Internet. It automatically encrypts messages, and it is possible to have multiple email accounts with only one click. It is the most secure way for communication, and its popularity is on the rise.

**How To Use I2P?**

The official I2P website is very techie-orientated, and in our view it doesn't do a good job of explaining in simple, newbie-friendly terms.

Therefore we composed a brief guide on how to use I2P, to get you up and running with the I2P Darknet in Windows (since that is the system we run). If security is a top priority for you, then you should not use Windows (or OSX), instead opting for a Linux distro (and preferably a security-oriented one such as Tails or Liberté Linux). Even better, use  Ipredia OS, a Linux distro based on I2P, with websites and services only accessible through an I2P proxy tunnel.

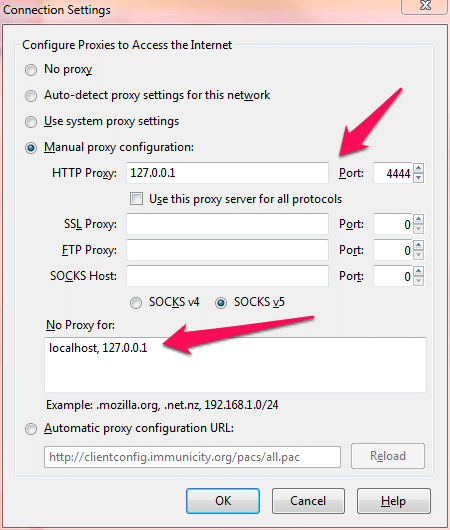
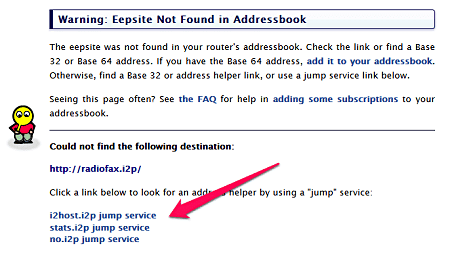
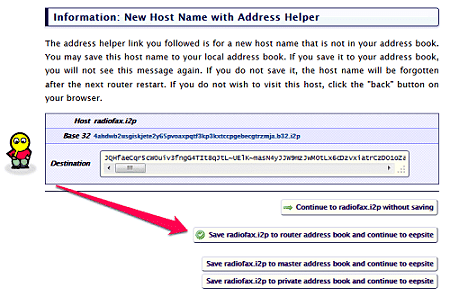
**How To Set Up And Connect**

1. [Download and install Java](https://www.java.com/en/download/) –I2P is written in the Java programming language, so to run it you will need to have Java installed. It is quite likely that you already have this on your system, but if not, then download the latest version and install it (if you are not sure then skip this step for a minute, and come back if I2P refuses to run).
2. [Download](https://geti2p.net/en/download), install and run I2P.
3. When you run I2P, a console window will open. If you need help, then you can copy and paste the log files from here, which will be useful to anyone assisting you.  
   
4. A browser window will also open on the I2P Router Console page to let you know that you have connected successfully to the IP2 network. You may initially have to wait a few minutes while the software finds peers and connects tunnels to them.  
   
5. Once done, the Router Console will show that you are fully connected.  
   

**I2P Browser**

In order to browse eepsites in the I2P network, your browser must be configured for that purpose. On the I2P website you can also find [a useful guide](https://geti2p.net/en/about/browser-config) for the configuration settings of some popular browsers like Internet Explorer or Firefox.

It can be done in any browser, but as we consider Internet Explorer to be insecure, and Chrome an open window for Google spying, we will use Firefox (the process is similar regardless of browser).

1. Go to Firefox -> Options -> Advanced tab -> Network tab -> Connection Settings.
2. Check the ‘Manual proxy configuration’ box and enter the following values: HTTP Proxy: 127.0.0.1, Port: 4444. It is also a good idea to add ‘localhost, 127.0.0.1 to the ‘No Proxy for’ box.  
   
3. OK your way back out of Settings and you are done!
4. It is commonly recommended that you use the Firefox Extension "FoxyProxy" to change proxy settings quickly if you use I2P often. That is a great idea, but we experienced connection problems when we tried it (which may be the fault of our highly kinked Firefox browser).
5. You should now be able to connect to I2P websites, known as eepsites which have the .i2p suffix. Enter the address of any eepsite (one of the .i2p links in the Router Console window is a good place to start).  
   
6. At first, you will not have any eepsites in your router’s Address book so you will need the help of a ‘jump’ service. The reasons for this are somewhat technical, but all you need do is click one of the jump service links. If a link doesn’t work, try another (we had much better luck using the second link down).  
   
7. Click on "Save [website] to router address book and continue to eepsite", and the eepsite should load. Unfortunately, when you first start using I2P, you may have to go through this process a few times.

**I2P Ready To Use**

You should now be connected to an eepsite, and are ready to explore the I2P darknet. A good place to start finding new eepsites is the eepsite.com search engine. Enjoy!

A great deal of information (including info on configuring firewall ports) is available from the main website but is beyond the scope of this beginners guide. If you have further questions about I2P, what it is good for, and what alternatives are out there, then read on!

**Be secure on the dark web**

We recommend that you use a VPN service before downloading encrypted browsers I2P or Tor in order to cover your tracks. Find out more in our [best VPN for the dark web article](https://proprivacy.com/vpn/comparison/dark-web-vpn).

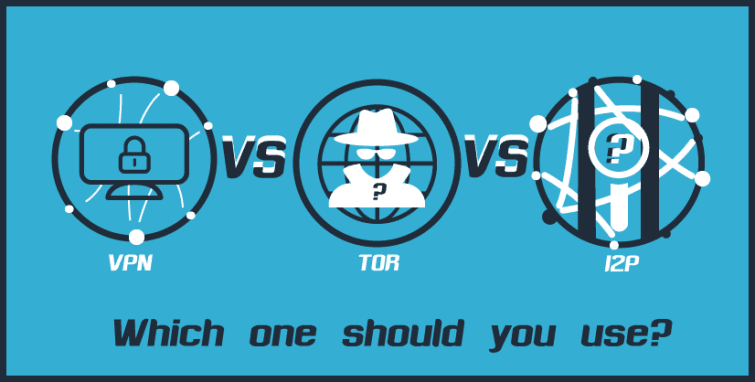
**Tor**

Tor sits in a slightly odd position, as it was designed primarily to access the visible internet anonymously. That, however, is one of its primary weaknesses. There are a limited number of exit nodes, which makes it easy to block these exit nodes, to set up ‘honeypot’ exit nodes to monitor traffic (although the way in which the [onion router](https://proprivacy.com/vpn/guides/tor-vs-vpn) works should still ensure that the end user remains anonymous), and to perform [‘end-to-end-timing’](https://proprivacy.com/vpn/comparison/5-best-vpns-when-using-tor) attacks to uncover the identity of Tor users.

In response to this, Tor has developed its Hidden Services protocol, which allows Tor-only websites (.onion) and services to exist entirely within the Tor network so that users do not have to access the visible web through potentially dangerous exit nodes at all. Tor Hidden Services therefore also acts as a Dark Web and is by far the most popular such service.

However, because Tor was not originally designed as a darknet, alternatives such as I2P and Freenet, which were created from the ground-up as darknets, offer distinct advantages.

**VPN vs. Tor vs. I2P – Which one should you use?**



The simplest answer is that it depends on what you want to do. Fortunately, nothing is stopping you using all three depending on the task at hand, which is the approach we would advocate.

**VPN**

For general internet use,VPN is fast and easy to use, while providing a high degree of privacy. We firmly believe that people should VPN all the time by default to prevent dragnet surveillance by the likes of the NSA. It is also ideal for P2P downloading.

**Tor**

If you need to interact with the outside world as anonymously as possible then Tor cannot be beaten. For example, if you are a whistleblower and want to contact a journalist. You can add further layer of anonymity by connecting to Tor through a VPN service.

Although Tor Hidden Services are not as secure or fast as I2P, their relative popularity can make them more fun and it may be important to website owners looking for visitors. It is also older, has more developers, and is better funded.

**I2P**

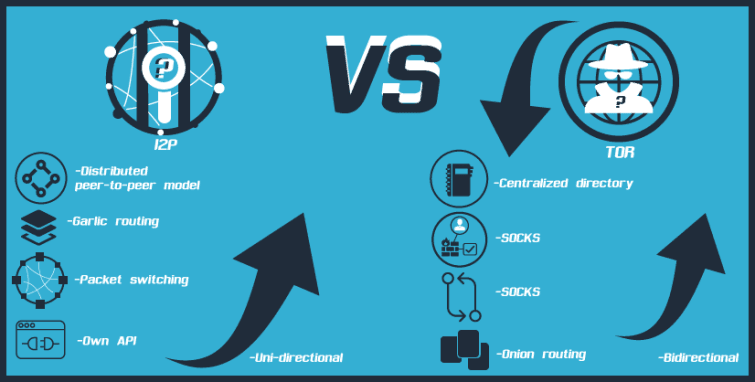
Technically it is the superior option if you want to access the Dark Web, and is our tool of choice for this. Although not as popular as Tor Hidden Services, it is still very sociable (and much more so than rival Freenet), and is an excellent choice for P2P downloading. Like Tor, it is a good free option for accessing the visible web anonymously for free (and maybe faster), but the limited number of outproxies mean that it is also much less anonymous when used in this way.

**VPN and Tor**

VPN and Tor are two ways to stay anonymous and preserve your privacy when online. Each has its strengths and weaknesses, which we discuss in some detail in this article. The bottom line is that Tor is extremely secure but very slow and unsuitable for P2P downloading, while VPN is less secure because it relies on trusting your VPN provider, but is much faster, is excellent for P2P downloading, and generally provides a better web browsing experience.

What both these technologies have in common is that they are primarily concerned with accessing the publicly indexed ‘visible’ (or ‘surface’) web.

**I2P vs. Tor**



* While Tor uses a centralized directory to manage the overall ‘view’ of the network, as well as gather and report statistics, I2P uses a distributed peer-to-peer model
* Unlike Tor Onion routing, I2P uses Garlic routing, which encrypts multiple messages together to make it more difficult for attackers to perform traffic analysis
* In contrast with Tor, I2P tunnels are uni-directional, so incoming traffic and outgoing traffic are completely separate, which improves anonymity
* I2P uses packet switching instead of Tor’s circuit switching, which means transparent load balancing of messages across multiple peers, rather than a single path. Essentially, all peers participate in routing for others
* I2Ps uses its own API rather than SOCKS which is used by Tor. This helps to make I2P more secure than Tor.

As with Tor, users of I2P connect to each other using peer-to-peer encrypted tunnels, but there are some fundamental technical differences.

Just as Tor is primarily a tool designed to access the visible web anonymously, but which can be used as a darknet, I2P is a Dark Web tool that can also be used to access the surface web anonymously through Outproxies (which are equivalent to [Tor Exit Nodes](https://proprivacy.com/vpn/guides/tor-vs-vpn)). However, I2P Outproxies suffer similar weaknesses to Tor Exit Nodes, and the fact that there are far fewer of them (as I2P has a much smaller user base) means that they are potentially more open to attack.

**Using I2P Conclusion**

We hope that you have all the information and knowledge you need regarding I2P! One thing to note is, just as with VPN and Tor, I2P does not hide the fact that you are using the service, but does make it very hard to discover what you get up to when connected to it. The result is that if using hidden services, I2P is both much faster than using Tor (it was designed with P2P downloading in mind), more secure, and more robust.