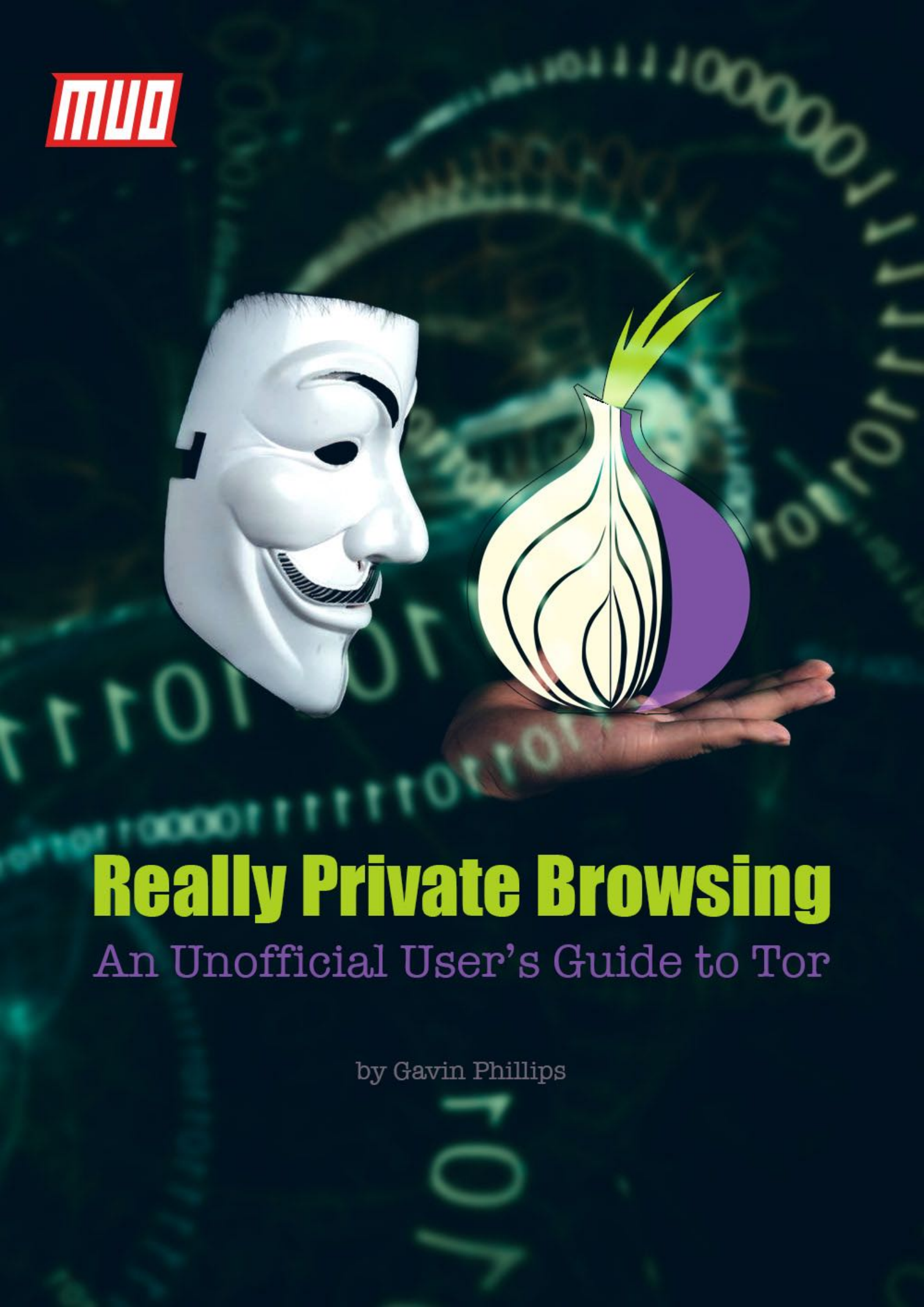

MUO
Really Private Browsing
An Unofficial User's Guide to Tor
by Gavin Phillips

Really Private Browsing: An Unofficial User's Guide to Tor

Written by Gavin Phillips

Published July 2017.

Read the original article here: **http://www.makeuseof.com/tag/really-private-browsing-an-unofficial-users-guide-to-tor/**

Table of contents

Privacy on the internet is a constantly evolving battleground. And for good reason. Revelations concerning government spying programs, almost daily data breaches, and less-than-transparent corporations are *de rigueur*. Tin foil hats abound; more and more citizens around the globe are taking note of their privacy… and where it is going.

When Edward Snowden revealed the PRISM (NSA) and Tempora (GCHQ) global surveillance programs, shock was met with apathy. Those that suspected this level of surveillance found their suspicions vindicated. But the average man or woman on the street? Many didn't even pause for thought. This sort of invasion of privacy makes a number of people very nervous; they're not just criminals, dissidents, and terrorists, either. **This level of surveillance directly affects everyone**.

There are a number of tools focused on protecting the privacy of regular citizens, like you and I. One of the most powerful tools at our disposal is **Tor.**

1. Let's Talk About Tor

Tor provides truly anonymous and untraceable browsing and messaging. Furthermore, Tor provides access to the so-called "Deep Web" — a network of untraceable, hidden websites providing everything from hard drugs to censored materials, and seemingly everything in-between.

Image Credit: g0d4ather vis Shutterstock.com

There are few **online privacy** methods as resilient and all-encompassing as Tor. Until **the FBI infected a number of Tor services with malware** (exposing their users and the service owners), the service was seemingly impenetrable. The military-grade encryption, combined with the Onion Routing protocol, made individual users incredibly difficult to trace. Even better, Tor is incredibly easy to use, created to be simple enough to use without a technical background. If you can download and install a program, you'll be able to use Tor.

In a nutshell, Tor is a powerful, easy-to-use piece of software that lets you keep your online life private. This guide will provide a step-by-step guide to installing, configuring, and using Tor.

2. How Tor Works

Tor was initially created by individuals "on contract from DARPA and the U.S. Naval Research Laboratory's Center for High Assurance Computer Systems." Indeed, most of the funding for Tor has come from the U.S. Government in one form or another.

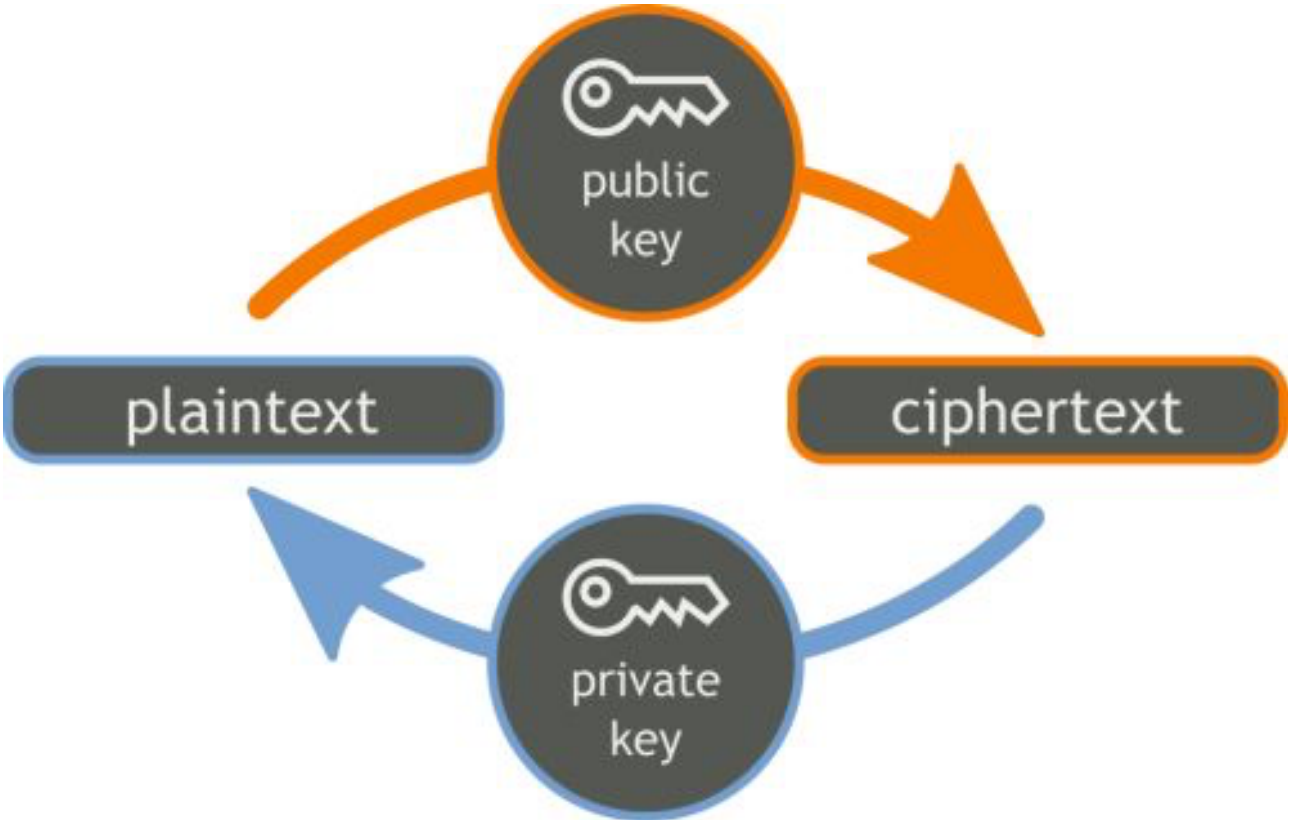
Tor is an acronym. It stands for The Onion Router.

One of Tor's major strengths is accessibility. It isn't necessary to understand the technology to use and benefit from it. However, I'm going to explain how it works in this section because it is actually quite interesting. If you're not interested in the technical details, feel free to skip to the next section on **Installing the TOR Browser Bundle**.

2.1 Modern Cryptography in Brief

Most modern cryptographic tools use **asymmetric encryption**. Asymmetric encryption allows you to use two different "keys" to encode and decode information. Here is the clever bit: the encoding and decoding key are linked so they only work with one another. However, there exists no efficient way of uncovering one key given the other.

Consequently, you can distribute your encode key — typically referred to as a "public" key — while keeping the matching decode key — the "private" key — secret. In turn, this means that anyone who wants to communicate with you in secret can use your **public key** to **encode** a message. When the message arrives, you use your **private key** to **decode** it.



Any communication taking place using Tor utilizes HTTPS. In practice, this means you and the person/site/service you're communicating with initially exchange your public keys; this allows both of you to talk to the other securely (even over a tapped line). A third-party listening in would see the public key exchange. But everything after that would be undecipherable gibberish that they cannot decode.

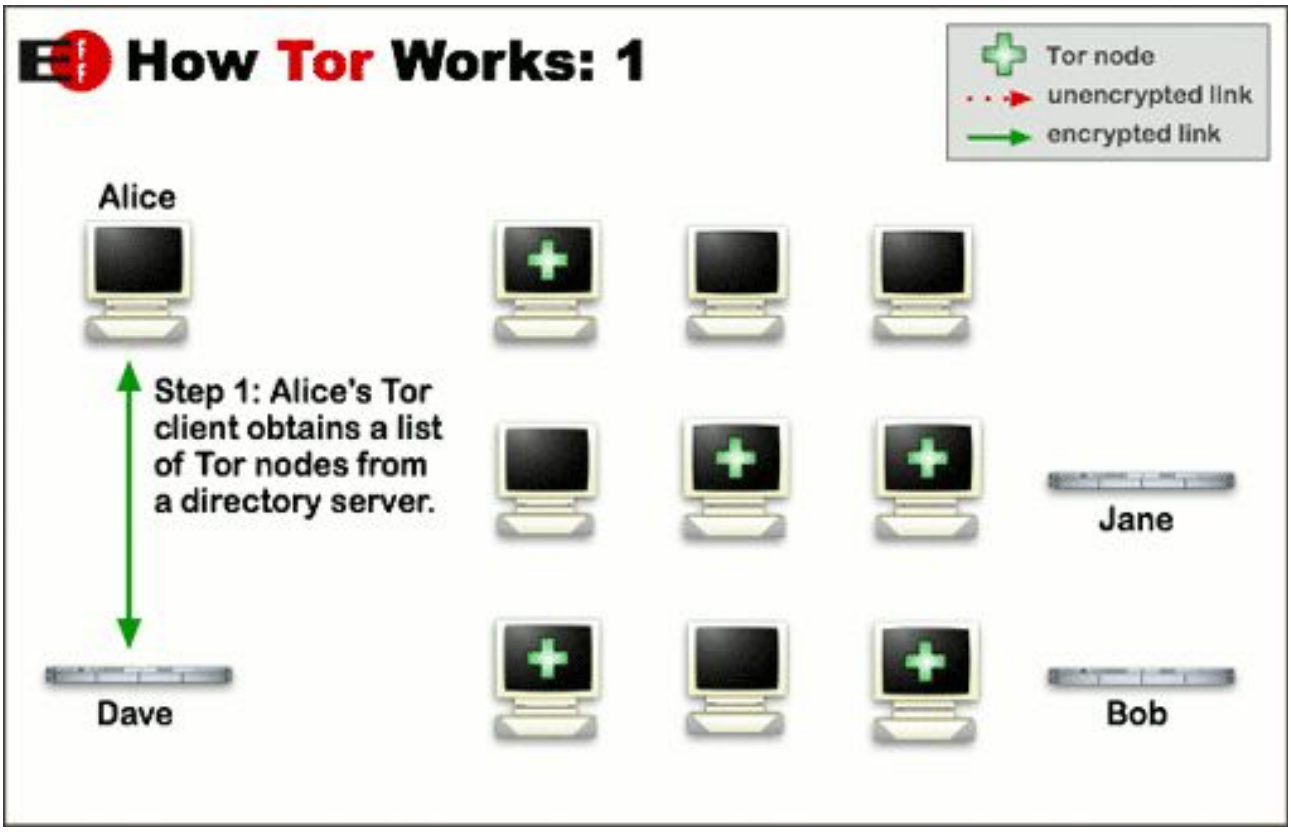
Sounds good, right? Tor takes this even further using the onion routing protocol discussed above.

2.2 Onion Routing: Not Just for Vegetables

Even if two people are talking in a language you don't understand, you can still deduce a lot by watching who talks to who. That's where onion routing steps in. Onion routing is as it sounds: routing through many layers, like an onion. This process obscures the message content, as well as where the message has been and is going.

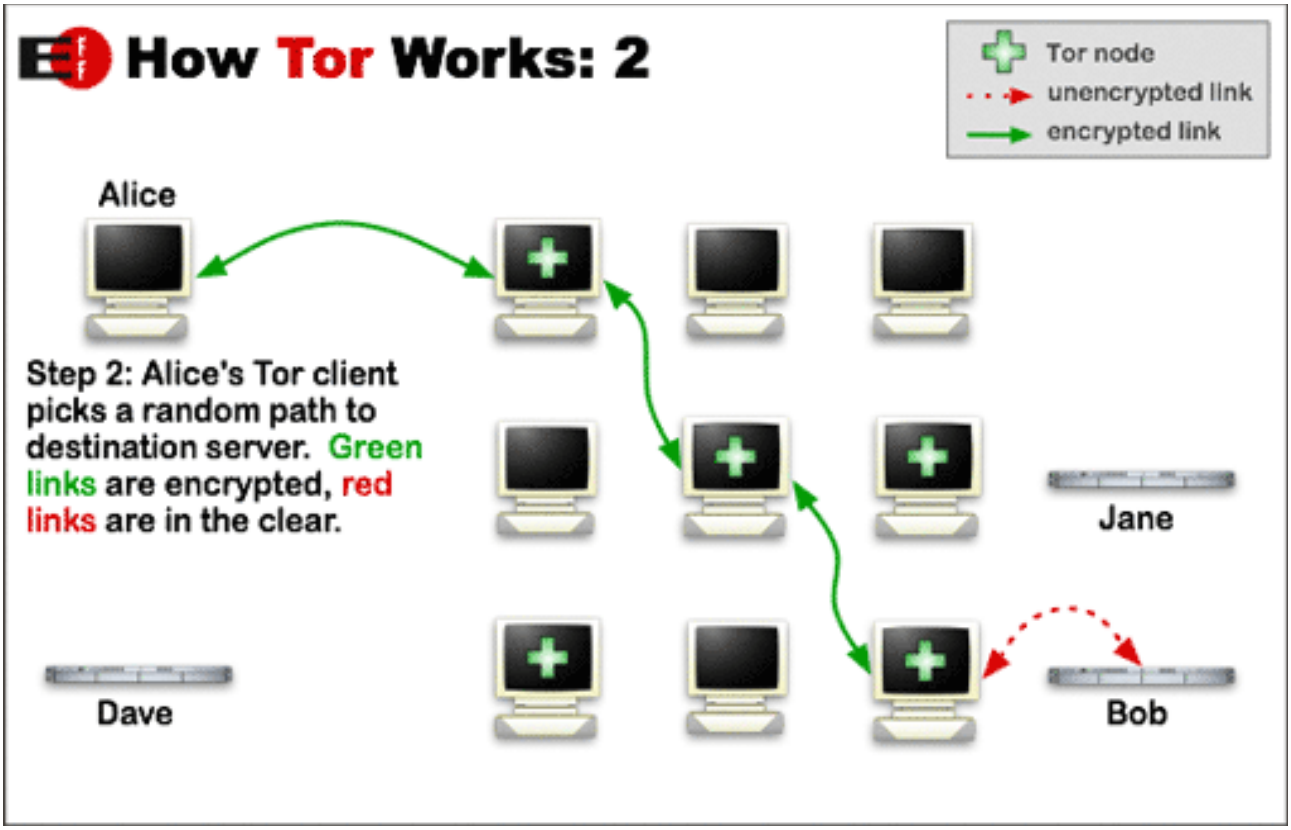
To understand how Tor keeps your identity private, it is necessary to understand a few underlying principles.

- All Tor users distribute a copy of their public key and IP address using an integrated peer-to-peer network.
- Tor network anonymity uses a system of relays, also known as nodes. The more nodes that are running, the more robust the Tor network is.
- The only piece of data decrypted in transmission is the forwarding IP address.
- Received data carries the IP address of the "exit node" — the final link in the encryption chain
- While Tor is an excellent anonymity tool, the exit node **can be compromised**.



Bearing those things in mind, the following is an abstract example of how sending a private and encrypted message on Tor actually works.

1. You open your Tor-enabled browser (client). The client encrypts all data packets sent from your computer.
2. Your computer sends a data packet to Node A.
3. Node A encrypts the already encrypted data packet, and sends it to Node B.
4. Node B encrypts the already encrypted data packet, and sends it to Node C.
5. This cycle continues until the data packet reaches Node Z — the “exit node.”
6. Node Z decrypts all the layers of encryption on the data packet, and delivers it to its final destination.



And when someone returns your message, it follows the same process, albeit via a different route. The multiple layers of encryption make decrypting intercepted (sniffed) data packets extremely difficult. The data transmits in a vault within a vault within a vault within a vault, and so on.

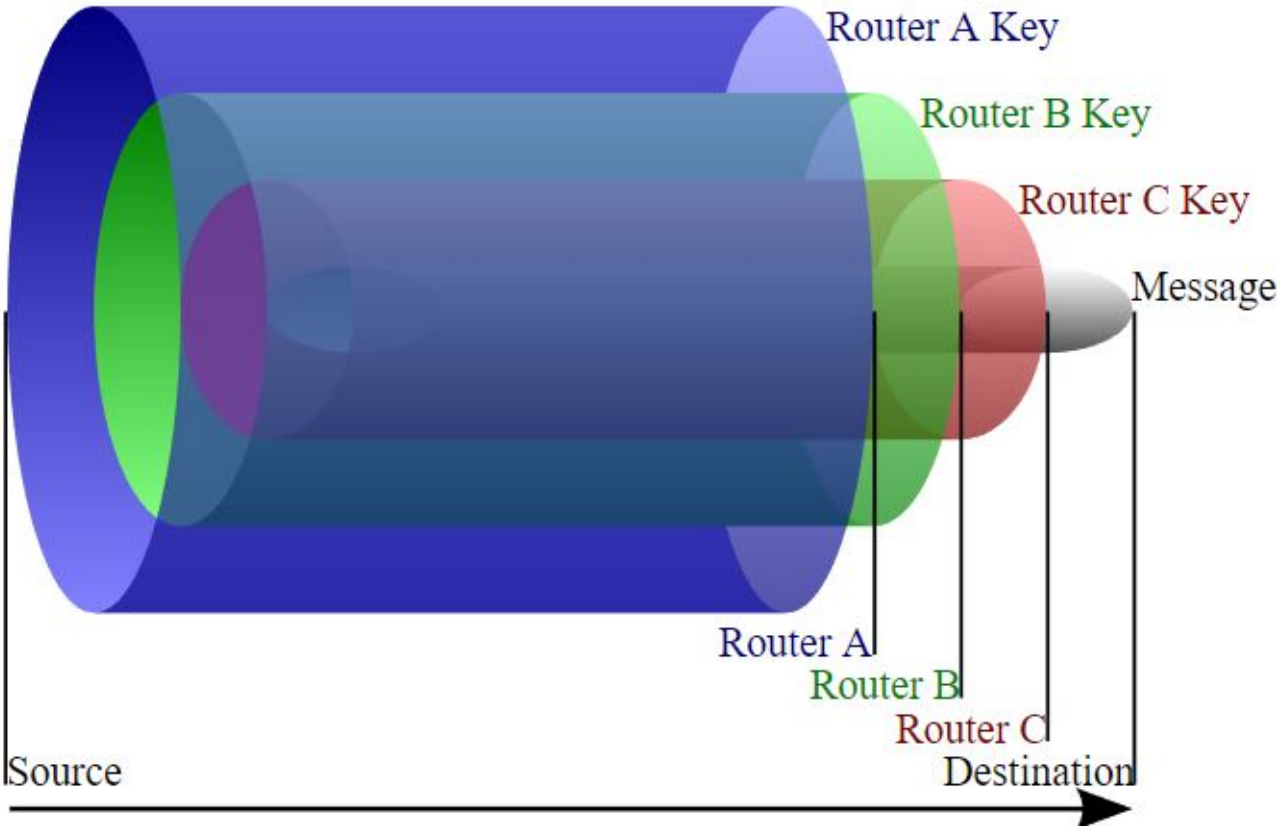
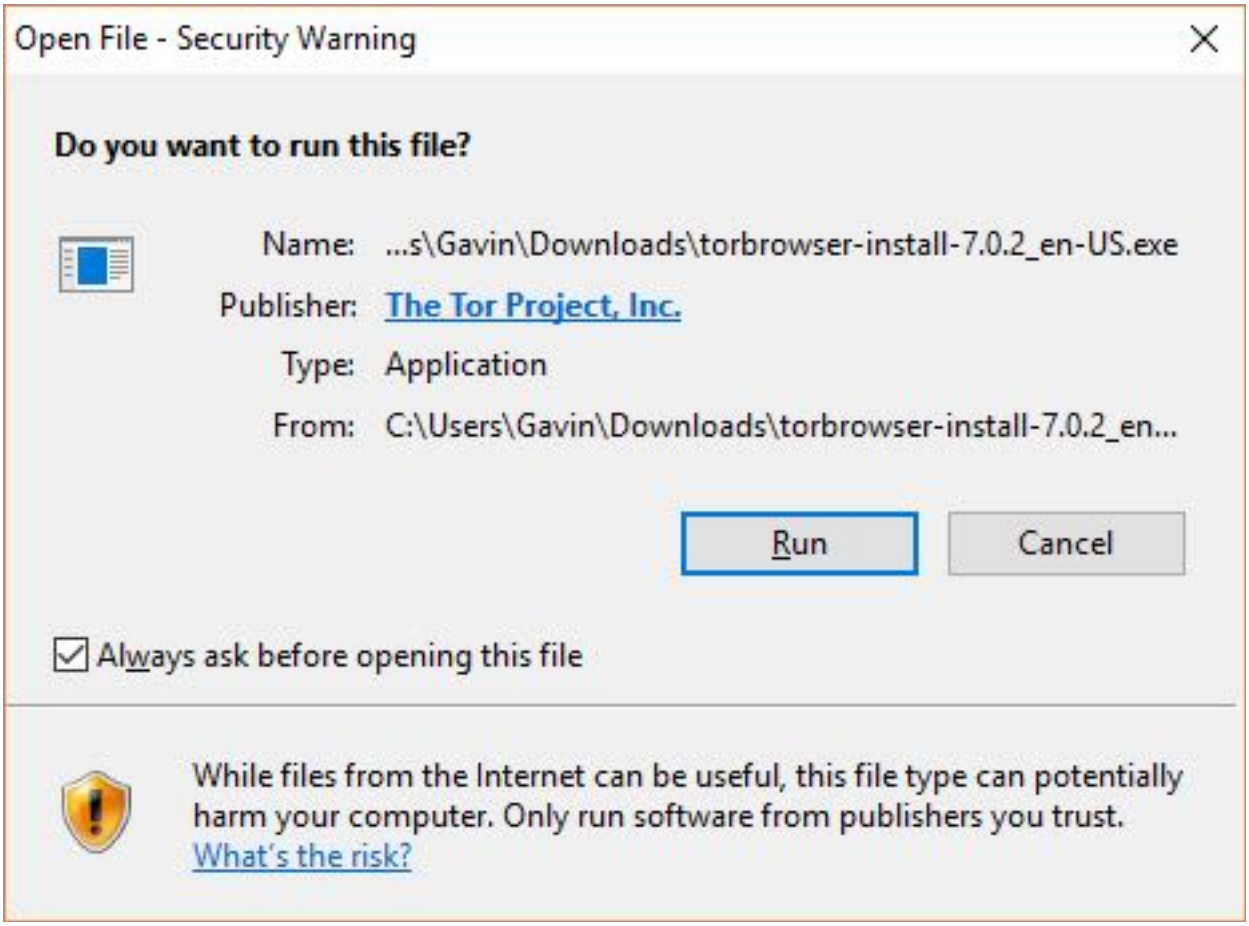


Image Credit: **Harrison Neal** via Wikimedia Commons

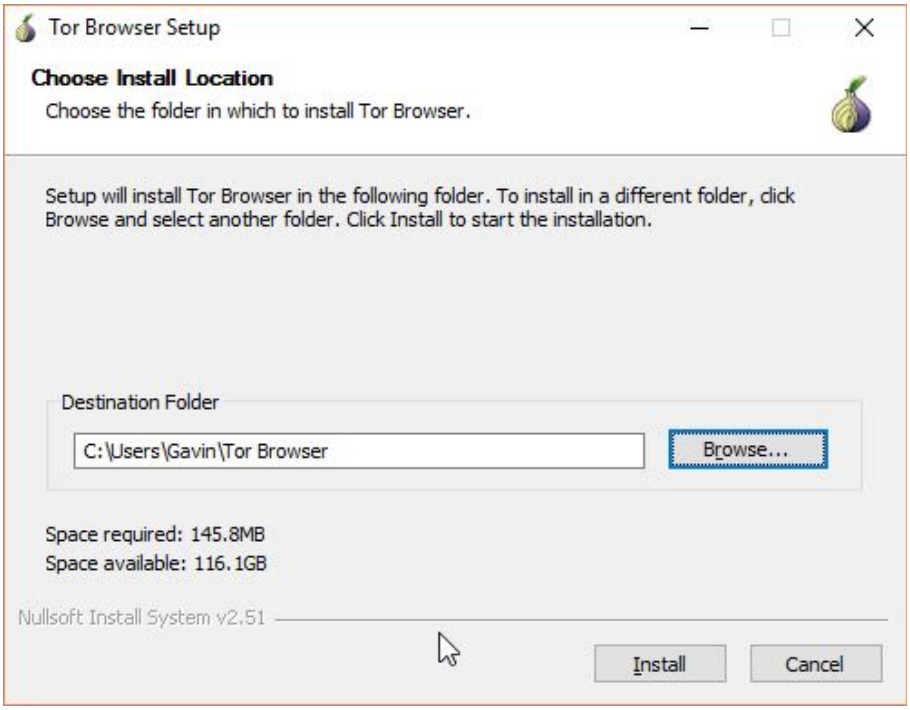
3. Installing the TOR Browser

Installing Tor Browser is easy. It's available for Windows, Mac, and Linux, but we'll go through the process for Windows. First, head to **https://www.torproject.org/** . The 's' after 'http' is important, as it means (among other things) that your computer is verifying that the website you're talking to is what it claims to be. Then, click the large **Download Tor** button, and, when the website loads of new page, click the large **Download Tor Browser** button. (**Tor isn't the only browser focused on privacy**… it just does a lot more than the others.)

The download will begin. On completion, head to your download folder, and run the installer. If a Security Warning appears, select **Run**.

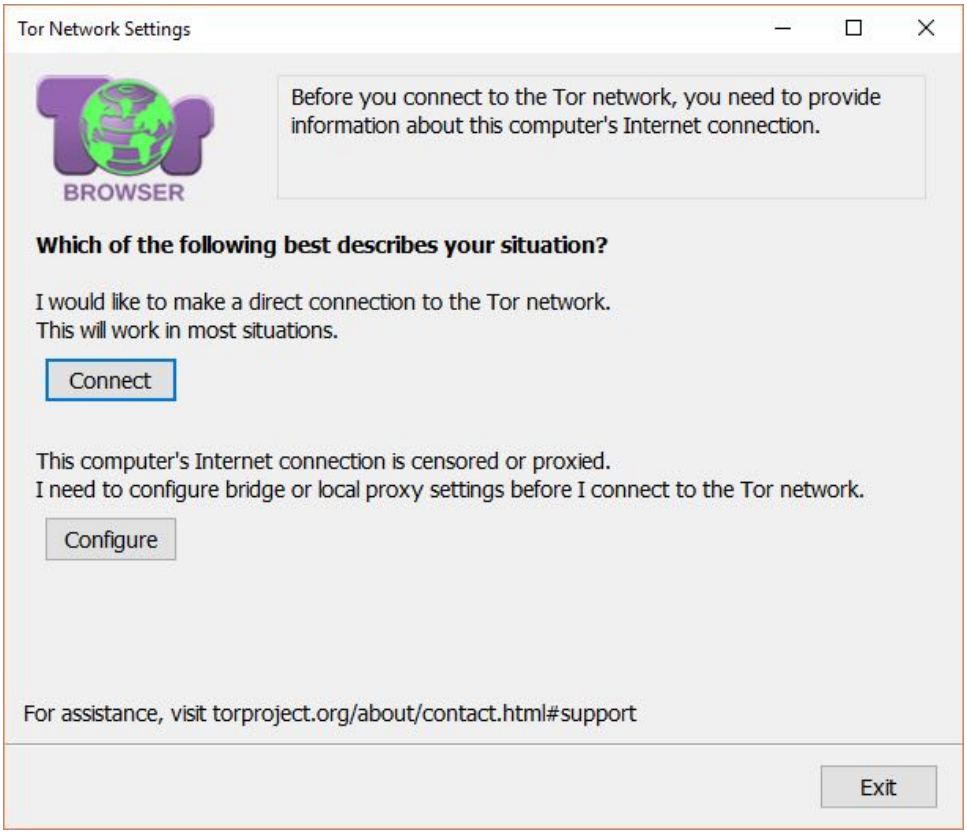


Select the language you'd like, followed by the directory where you'd like to install the Tor Browser. Select **Install.** The browser will now extract and install. On completion, you'll have two options: **Run Tor Browser**, and **Add Start Menu & Desktop Shortcuts**. Ensure both of these are checked, and select **Finish**.



3.1. Tor Browser Network Settings

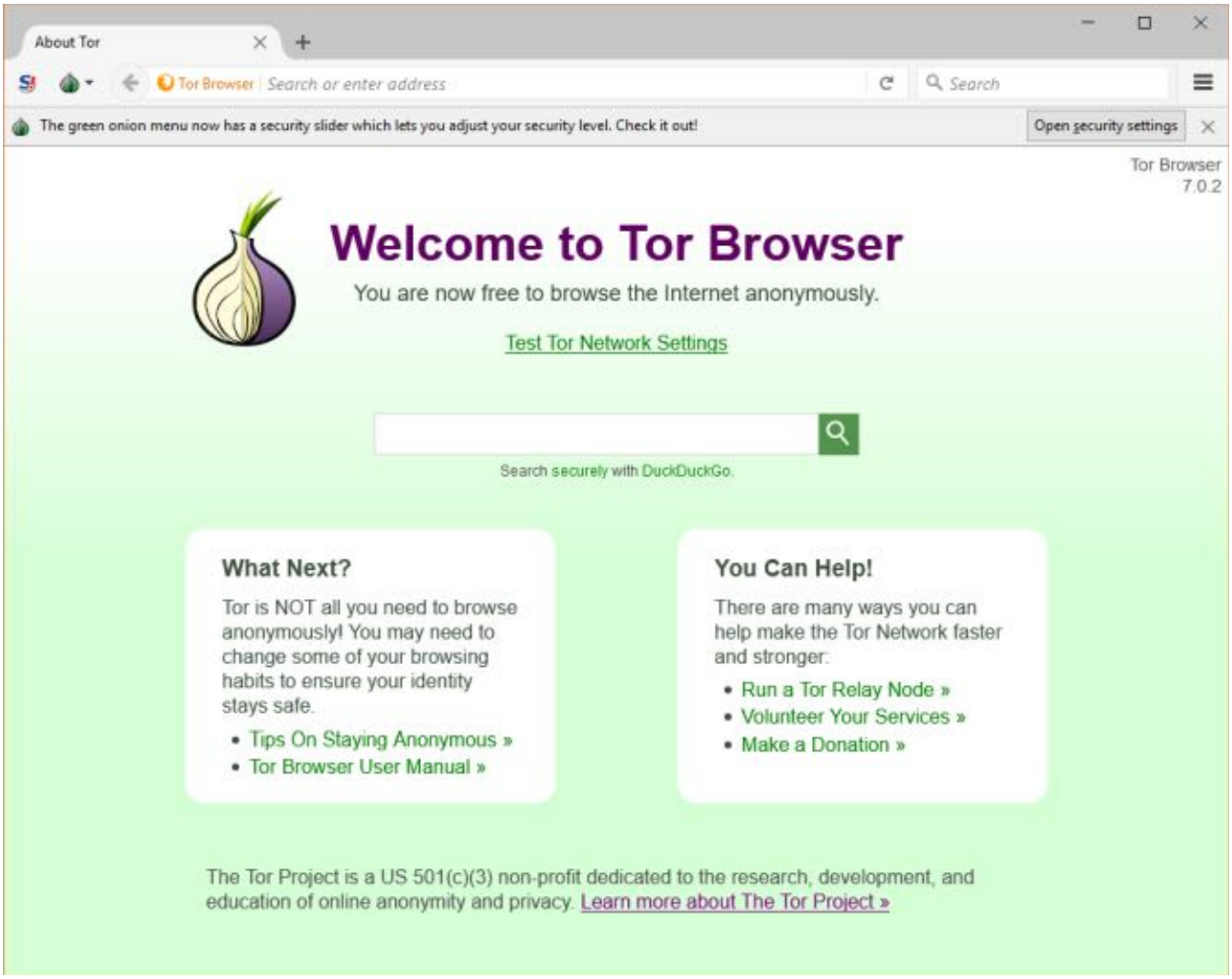
When you open Tor browser for the first time, you'll need to select your network settings. In this instance, select **Connect**. (We'll explore the **Configure** button in a moment.) You'll spot a small loading bar. You'll arrive upon the Welcome to Tor Browser page when it completes.



If the client requires an update, do so before moving on. This is very important. If not, please head on to the next section of the tutorial.

4. Using Tor Safely

One of the things you'll immediately note is the Tor browser's similarity to Mozilla Firefox. Tor browser is based on Firefox, but features the TorLauncher, TorProxy, and the TorButton, as well as the **NoScript and HTTPS Everywhere Firefox extensions**.



For the most part, it is a completely normal browser. That said, you'll have to slightly tweak the way you browse, and **you might find some of your most used features "broken."** (This is due to the limitation on trackers and scripts). Tor protects your privacy out-of-the-box.

4.1 Tips for Safe Browsing

Tor does an enormous amount of leg-work on the privacy front. But if you want it to be completely effective, you'll have to adjust the way you use the internet.

A good start is being aware of the *limitations* of Tor and the Tor browser.

- **Tor is not a VPN. Tor is a proxy.** It only protects traffic routed through the Tor browser.
- Tor cannot protect you if the person you're communicating with is taking a physical log. It can protect your IP address and, if you use a pseudonym for anonymous communication, your identity will be protected, too.

- Tor cannot control the actions of third-party browser extensions, hence their very strong suggestion that you don't add any to the base installation (unless you really know what you're doing). Both malicious and non-malicious extensions can reveal your identity without you realizing.

- Tor cannot strictly enforce HTTPS. The HTTPS Everywhere extension attempts to force HTTPS support on every site, and while many sites support the standard by default, Tor cannot take account for those that don't.

In addition, Tor doesn't connect to Google, by default. Google keeps **extensive logs on all searches made using it**, as well as tracking your in-browser internet activities. There are arguments against Google tracking, and of course, arguments for. Regardless, the Tor welcome page uses anonymity focused internet search tool, DuckDuckGo, by default. DDG search results are a compilation of "over 400 sources." Some users don't like the DDG search results, preferring to use StartPage instead (StartPage acts more as an anonymizing proxy delivering actual Google search results).

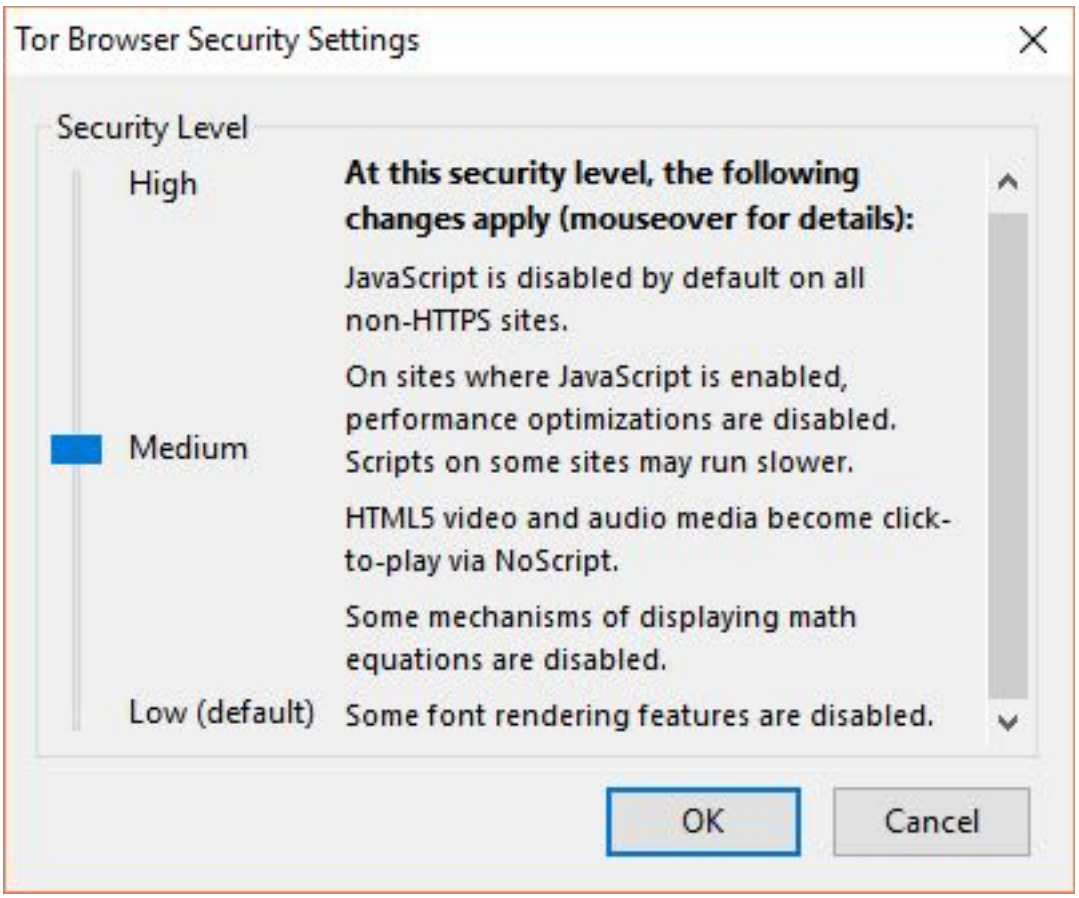
One of the side-effects of these privacy measures is that some sites will not work, while others will require additional sign-in verification. Notable sites include YouTube, some airline sites (they **love** tracking you!), online banking portals, and more. Furthermore, any site that relies on Flash will cease to function, as Tor steers well clear of that security and privacy nightmare. (This problem is slowly alleviating as more sites switch to the vastly more secure HTML5).

Finally, there are a number of document types that can contain resources that circumvent Tor. These files — for example, an .exe, PDF, or .doc — may innocently disclose about your browsing activity. As with most modern browsers, Tor will offer a warning when you download a potential security risk. In this case, it is wise to pay attention.

5. Configuring Tor

As stated in the previous section, Tor protects your privacy out-of-the-box. You don't need to fiddle with security settings, or download additional extensions to begin browsing the internet anonymously. Tor once allowed all users greater autonomy in their access to security and privacy settings. Unfortunately, it meant a great deal of curious (and well-meaning) individuals actually opened themselves up to the internet, defeating the purpose of Tor. There is now a single security settings slider instead, keeping things extremely simple.

To change the security level, select the **Onion** icon alongside the address bar. It will open a dropdown menu; select **Security Settings**. You can then choose Low, Medium, or High security.



Low security (the default setting) enables all browser features, while still routing and encrypting traffic.

Medium security disables JavaScript on non-HTTPS sites, turns all HTML5 media into click-to-play (rather than autoplay), and disables some other scripts.

High security disables JavaScript on all sites, turns all HTML5 media into click-to-play, and disables a significant number of scripts. As such, some font rendering features will fail, as well as images and icons.

The level of security you require is, of course, subjective. If you're just looking to encrypt your browsing traffic, and be a little less forthcoming with identifying data on the internet, choose **Medium.** It strikes a happy balance between a comprehensive internet experience, and anonymity.

5.1 Using Tor in a Restricted Country

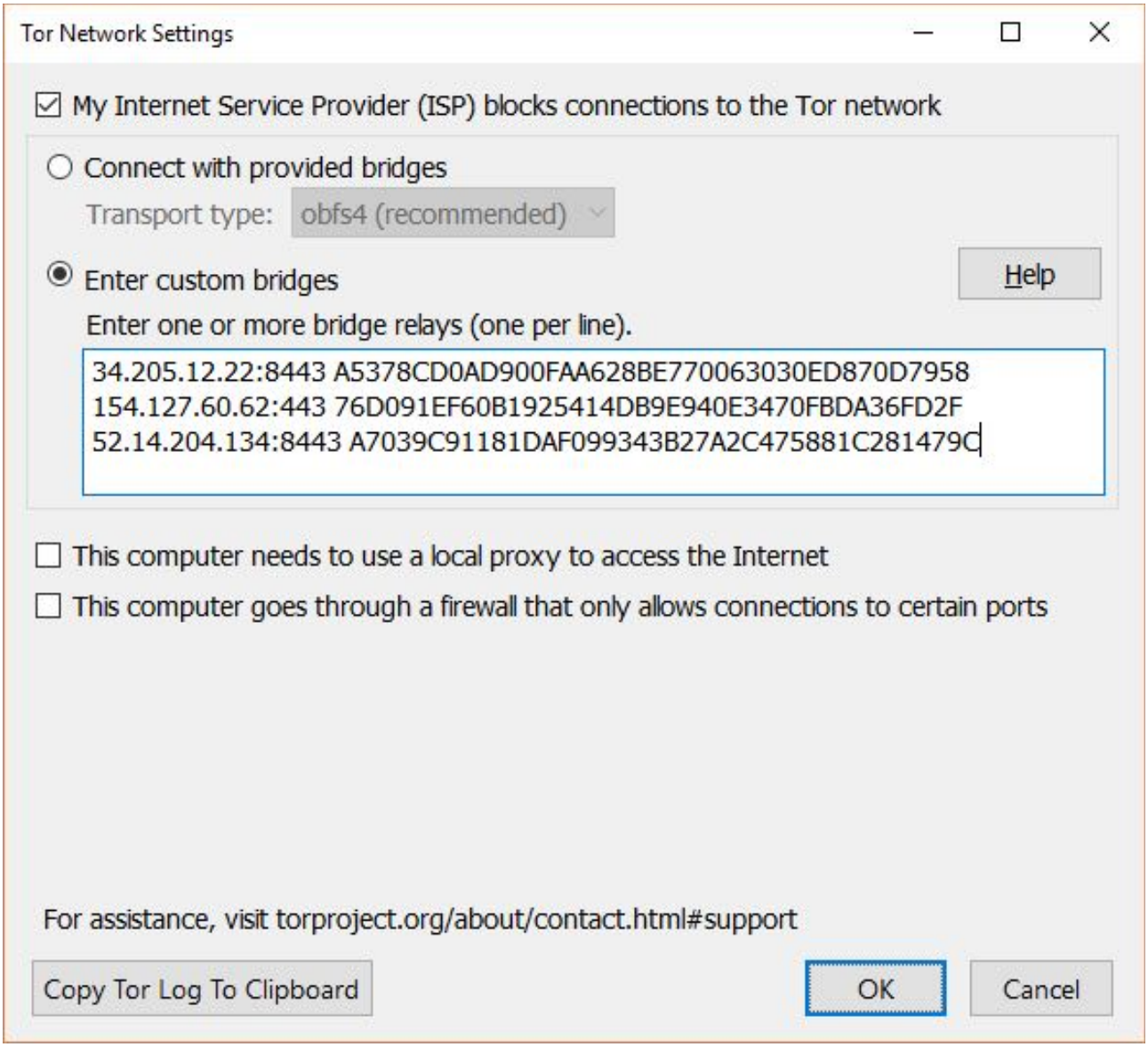
Of course, one of the major benefits of Tor is keeping your internet browsing private from an oppressive government regime (or otherwise). Unfortunately, censors have found ways to block Tor. In these cases, restricted users can use a **bridge**. A bridge creates an obfuscated relay on the Tor network that isn't listed in the main directory. The hope is that even if your ISP is monitoring all known TOR relays, they cannot block all the obfuscated bridges, in turn delivering an extra connection option to those in need.

To use a bridge, select the onion icon alongside the address bar, and select **Tor Network Settings.** Then, check **My Internet Service Provider blocks connections to the Tor network.** A new panel will appear. You now have a couple of options:

- **Connect with provided bridges**. The preconfigured Tor bridges are easy to use, and the majority of the time, will allow you to connect to the Tor network. However, because they are

easily accessible, there is a chance that they're already censored. **obfs4** is the current recommended bridge, but depending on your location, another option may work better.

- **Enter custom bridges**. If you know the address of a Tor bridge you'd like to specifically connect to, enter it here (one per line). If you don't know how to find a Tor bridge address, but you're sure you need one (autobridge settings don't work), visit bridges.torproject.org and follow the instructions.



5.2 Become a Node

By default, Tor will run in client mode, using the Tor network, but not actively contributing to its operation. This means your privacy is maintained, but other users cannot use you as a node. Which for the many, suits just fine. If you have a comfortable internet connection, however, you might consider contributing a small amount of bandwidth to the Tor network. It'll help keep the network operational.

Becoming a Tor relay is slightly more difficult than it used to be. Previously (I'm talking several Tor browser iterations back, now), there was a simple toggle to switch between client and relay mode. However, we'll show you how to do it manually. First up, this works best using an up-to-date Linux distribution. I'll be using Ubuntu 17.04 32-bit.

Start by installing the latest version of Tor Browser for Linux using the following command:

```
sudo apt install tor
```

Once installed, use a text editor to open the Tor configuration file. I'm using Vim.

```
sudo vim /etc/tor/torrc
```

Torrc is the Tor configuration file. The configuration file uses "#" to comment out potential commands. Deleting the "#" toggles the command. We need to enable the following commands:

- **#Log notice file /var/log/tor/notices.log** — turns on logging for your Tor relay
- **#ORPort 9001** — sets the Tor relay port. Change this to a port of your liking, but remember to update your firewall and router
- **#Nickname** — add a nickname for your Tor relay
- **#RelayBandwidthRate xxxx Kbytes** — sets the data rate for your Tor relay during non-peak times
- **#RelayBandwidthBurst xxxx Kbyte**s — sets the data rate for peak "bursts"
- **#AccountingMax xx Gbytes** — the amount data you can offer the Tor network. Switch to **Mbytes** or **Kbytes** if required. Threshold applies to incoming *and* outgoing e.g. if you set 5 Gbytes, up to 10GB is available

When you've set your data rates, save the configuration using the "**:x**" command. I've made a short video detailing the process, to clarify things.

Watch the YouTube video here: **Configure a Tor Exit Relay**

You can check the global Tor relay stats, including the Top 10 relays, over at **globe.rndm.de**.

5.3 Exit Nodes

Those who are more ambitious may choose to run a Tor exit node. The exit node is the final hop between the Tor network and your computer — you use one every time you use Tor. Exit nodes are absolutely vital to the operation of the Tor network but, unfortunately, there are some risks to running one.

Some jurisdictions will attempt to hold an Exit Node operator responsible for the data transiting their node. Unfortunately, this can include illicit activity like piracy, illegal black-market dealings, and more. I'm not going to advise running an exit node unless you're genuinely prepared for the serious consequences of doing so. If you do want to run a Tor exit node, please read the following documents before proceeding:

- **Tips for Running an Exit Node**
- **Exit Node abuse issues**
- **Typical Exit Node abuses**

Running an exit connection isn't a terrifying ordeal. But it does require extra precautions.

6. The Deep Web

We've touched upon the Deep Web a couple of times in this article, and you've probably heard about it in the news, too. It isn't as immediately peril-filled as some publications would lead you to believe. That said, certain precautions are necessary, and part of that is understanding how to find and use Tor Hidden Services.

To understand why hidden services are important, we should talk about **one of Tor's major weaknesses: exit nodes**. At the time of writing, there were **just under** 7,000 active relays.

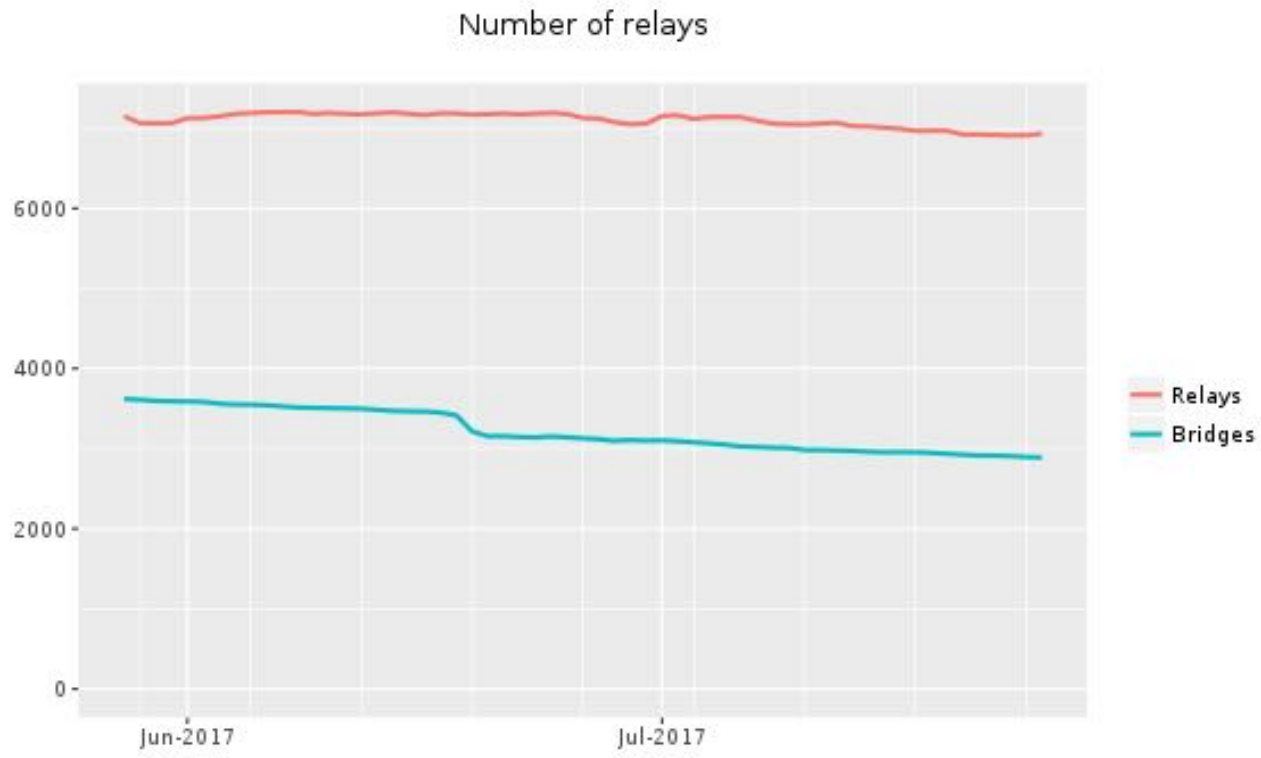


Image Credit: **The Tor Project**

Of those 7,000 relays, under 1,000 are exit nodes.

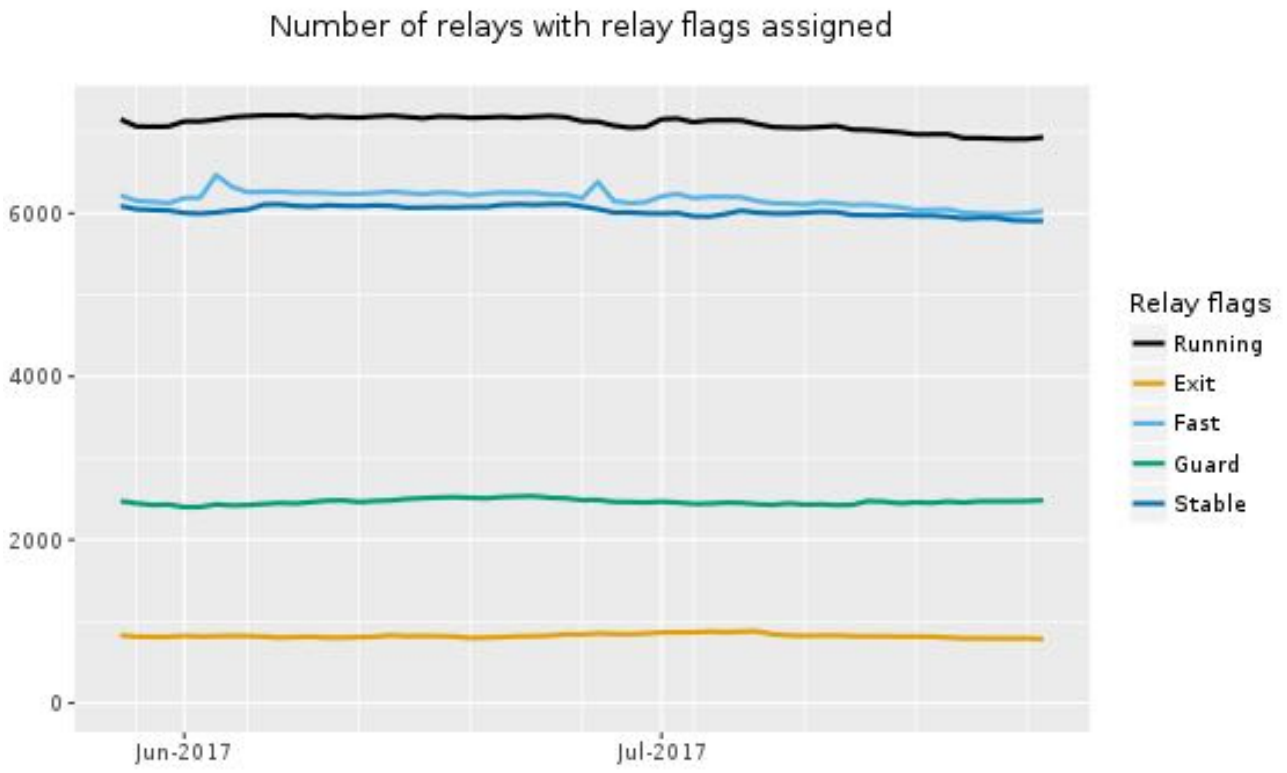


Image Credit: **The Tor Project**

Furthermore, there are over 2 million Tor users, sending traffic through those exit nodes. That traffic heads back to the "outside" internet. And **while HTTPS Everywhere encrypts your data**, once it leaves the Tor network, it is open to interception. If a single source can gather enough information about the flow of traffic through the network, it might be possible to deduce identifying information by completing timing analysis of the behavior of individuals, and the behavior of Tor exit nodes.

The top-level (sometimes referred to as the "clearnet" or "surface web") internet makes it very difficult to conceal both the physical location and ownership of a particular website server. Tor doesn't change that. The *viewer* is safely anonymous, but not the provider. This is where a Tor hidden service steps in.

A hidden service works just as a relay in the Tor network, but allows for the introduction of private, anonymous servers. When you access a hidden service, both you and the server are anonymous nodes on the Tor network. The traffic between you never leaves the Tor network and is therefore never exposed to prying eyes. In addition, understanding the physical location of a hidden service is equally difficult (though not impossible). Server anonymity makes serving subpoenas, blocking, or even removing a service extremely difficult. This is the reason there are some dubious and notorious Tor hidden services.

6.1 Deep Web, Dark Web, or Darknet?

The Deep Web is vast. But the majority of it is useless. **Or, rather, useless to you and I**, filled with millions of archives, web-service back-ends, databases, bots, and much more. There are **several specialist search engines** that can delve into the Deep Web. There is a little confusion surrounding Deep Web terminology.

- **Deep Web.** The deep web, as mentioned above, is a place full of unindexed databases, private networks, search engine crawlers, botnet command and control servers, and more.

- **Darknet.** A darknet is something like Tor: an encrypted network built on top of the existing internet, only accessible using special software. Other darknet examples include I2P, Riffle, and Freenet.
- **Dark Web.** The dark web is essentially the "WWW" of darknets.

These terms are increasingly used in the correct context, but major publications still, at times, use deep web, darknet, and dark web interchangeably.

6.2 Tor Hidden Services

It should go without saying that due to the nature of Tor, and the protections offered to hidden services, some extremely unscrupulous individuals and groups lurk there. It is easy to stumble across any number of things: drug dealers, pedophiles, terrorists, dissidents, hardcore fascists (and antifa)… the list is basically endless.

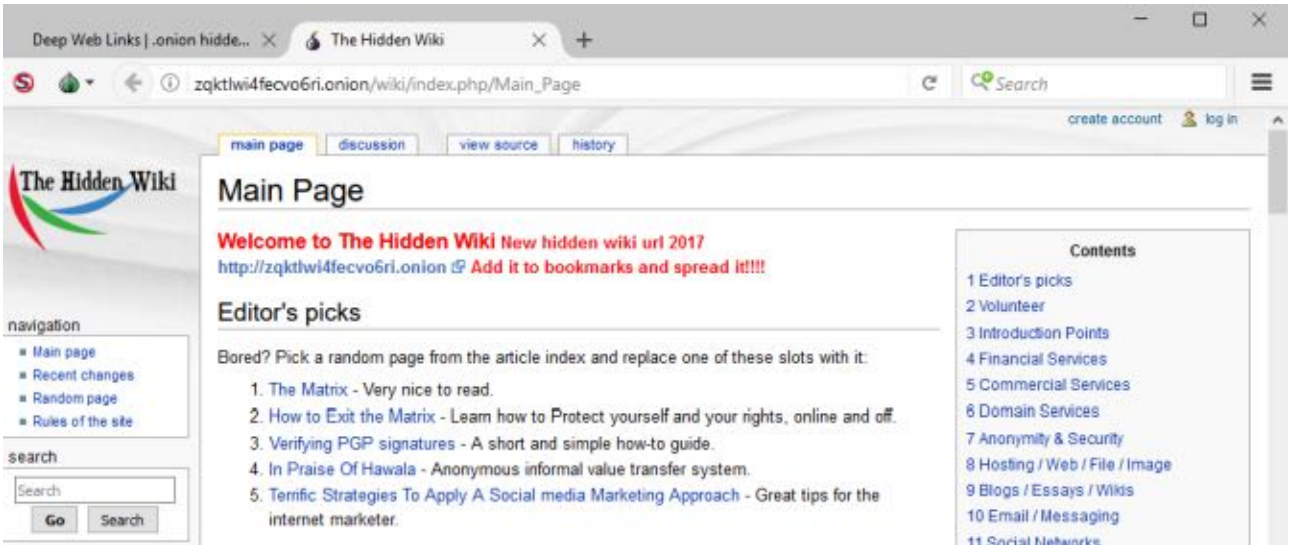
Watch the YouTube video here: **TOR Hidden Services - Computerphile**

Just in case: the author and makeuseof.com do not endorse any illegal activity committed by the reader, of any kind. This is education on anonymity and privacy.

Tor hidden service addresses use the following format: **https://[16-character hash].onion**. For example, this is the *current* link to The Hidden Wiki (uncensored!):

http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page

Note this service isn't using HTTPS. Technically, it doesn't matter as The Hidden Wiki is a repository for other .onion links. You won't be entering or leaving any personally identifying information.



The .onion suffix is a special top-level domain that signifies an anonymous hidden service. The 16-character hash address is automatically generated, based upon a public key created when the service is configured. It can become more than a little tricky keeping track of .onion addresses, so we suggest bookmarking your favorites.

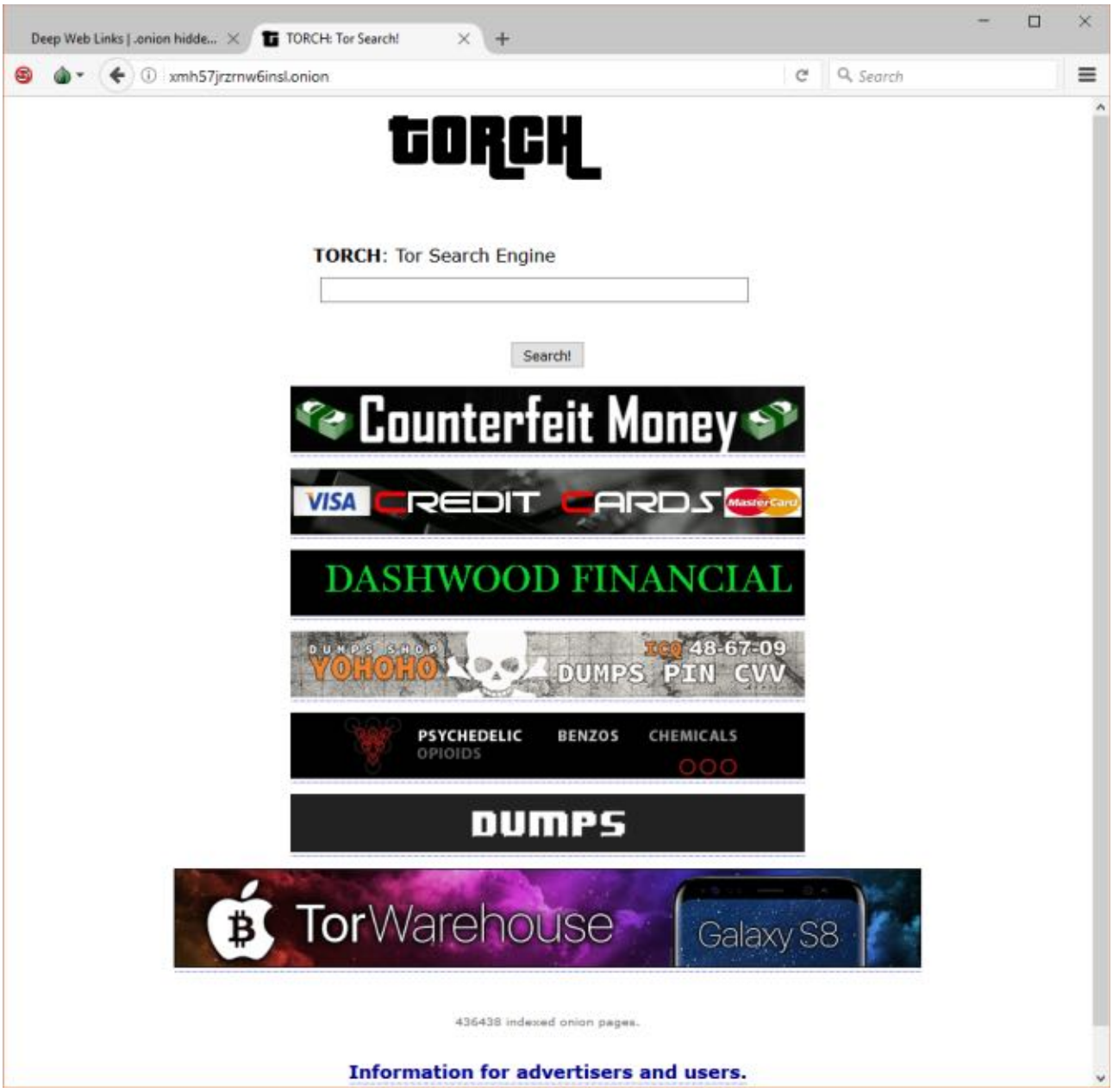
6.3 Useful .onion Starting Points

The Hidden Wiki is a pretty handy place to start your Tor experience. The service has gone through various guises over the years, not least because at one point it was compromised and redirected users to a malicious site. The link provided above is safe. But that could change,

given the nature of the service. Regardless, **The Hidden Wiki** archives and centralizes popular .onion links. It is somewhat moderated to remove some really horrific things, like illegal images of children, but you can rapidly find some pretty dark stuff.

As such, read the description of what you're about to click on.

Another extremely useful site is **Torch**. Torch claims to be the largest hidden service search engine, with over 1 million indexed results.



7. Anonymous Services

Out of the box, Tor allows you to browse the internet anonymously. Alone, this is extremely powerful, for users the world over. But beyond the immediate boost in privacy and anonymity, Tor hosts some pretty cool services, too. Here are three services you can use straightaway.

7.1 Anonymous Messaging

With the majority of global internet activity monitored and logged, an increasing number of people are turning to encrypted messaging services. Now, using Tor to chat isn't as critical as one was.

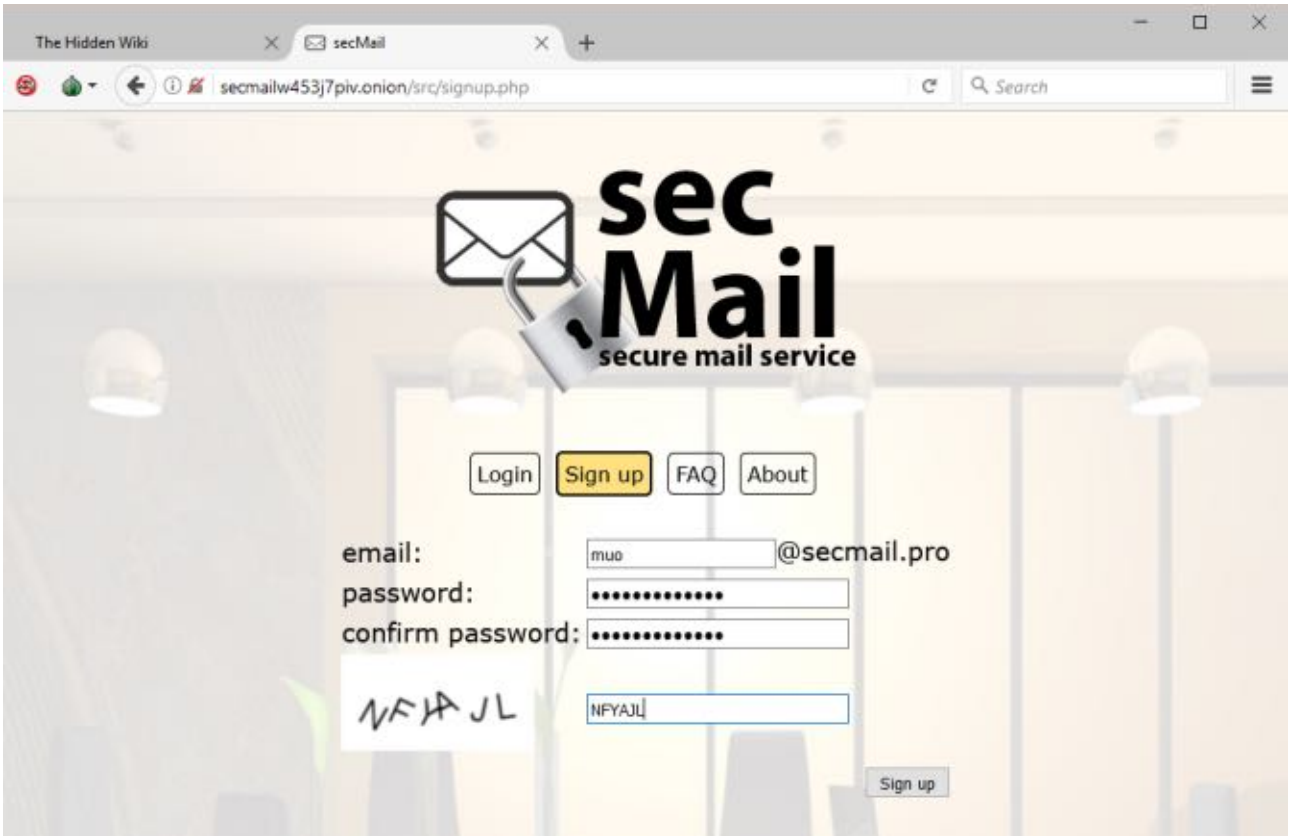
The advent of **mobile apps featuring end-to-end to encryption**, such as WhatsApp, Telegram, Silent, and Signal, have seen more "regular" users taking advantage of additional privacy (sometimes without even realizing!).

Bitmessage is an anonymous P2P messaging service that uses public key cryptography. Furthermore, they bunch encrypted messages together during the send process, before redistributing to the end user (not unlike Bitcoin tumbling). This makes it extremely difficult to decipher the source and destination of a single message. They have detailed **tutorials** on downloading, installing, and **configuring Bitmessage for Tor**.

7.2 Anonymous Email

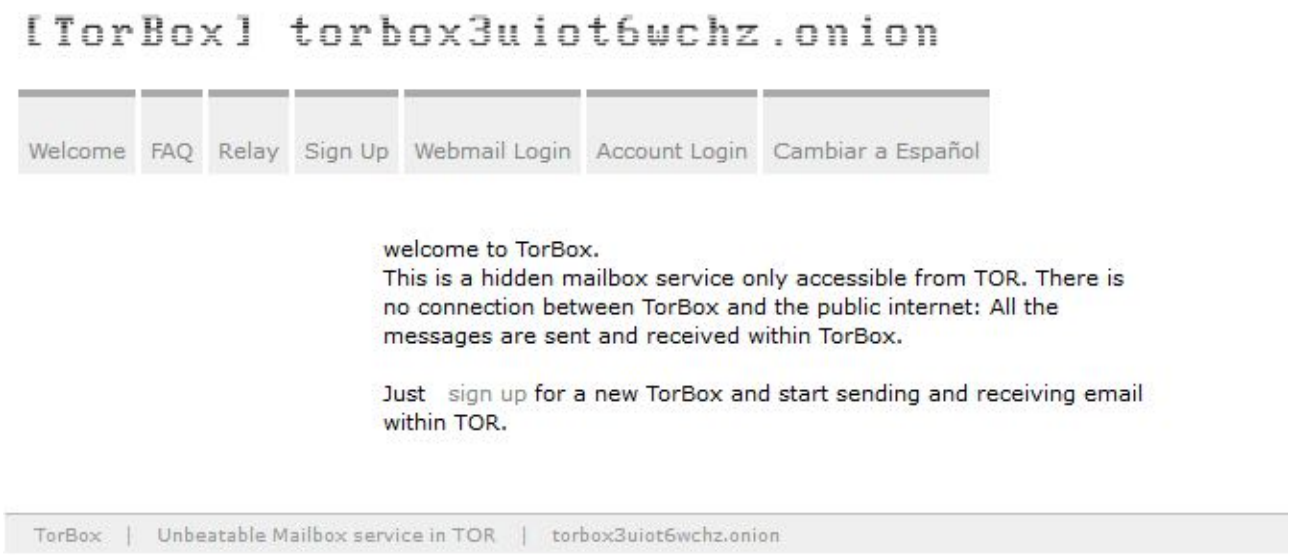
One of the most useful hidden services is fully anonymous email. There are only a few providers actually worth using, in that their service is consistent and actually functions.

One option is **Protonmail,** who operate a Tor login portal, **offering strong end-to-end encryption**. However, their servers are in Switzerland. And while Switzerland offers some of the strongest privacy protection in the world for individuals, they're not absolved. Furthermore, Protonmail requires JavaScript.



There is also **Secmail.pro.** Secmail is another hidden email service, using SquirrelMail. The service is relatively young (around seven months old at the time of writing), and as such, is still experiencing some teething problems.

Finally, there is **TorBox**. TorBox is available only through Tor, and can only send messages to other users within the TorBox service. In that sense, it keeps all TorBox mail and users extremely secure.



7.3 Bitcoin

Bitcoin and cryptocurrencies have flourished in recent years. This is in no small part due to their anonymity. As such, there are countless Tor services offering to duplicate, expand, and embiggen your Bitcoin wallet. The **vast majority are scams**. In amongst the scams, however, are some useful services. For instance, Bitcoins are largely touted as being completely

anonymous. But in reality, due to the blockchain record, tracing the users involved in an individual transaction is entirely possible.

If you want truly anonymous Bitcoin (and other cryptocurrency), they need tumbling. Tumbling is the crypto-equivalent of money laundering. It works (roughly) like so: you put your Bitcoin into a shared "pot" with other users. The tumbler assigns users the same amount of Bitcoins, but from a different initial user, breaking down or combining Bitcoins in the process. Everyone ends up with the same amount as they started.

Essentially, everyone switches coins, and everyone is a winner.

Many Bitcoin users are switching to **TumbleBit**, a new, open-source tumbler. TumbleBit is set to introduce full Tor support in 2017, and already has Hidden Wallet integration. Which leads me nicely onto…

Watch the YouTube video here: **TumbleBit is an anonymous payments system for Bitcoin**

The Hidden Wallet. The Hidden Wallet understands that privacy and anonymity breaking Bitcoin feature. As such, they offer cold storage security while tumbling your Bitcoin using their internal service. Their current tumbling charge is 0.001 BTC.

8. Support and Problems

Sometimes, software doesn't work. If Tor is giving you problems, there is a reason why. One of the first things to do is ensure you're using the most up to date version of the Tor client. Tor Browser checks for updates when you open it. If there is an update available, install it.

Next, check that your firewall or **router** isn't blocking Tor. You may need to setup port forwarding, or create a firewall exception. If you're still struggling, consider reinstalling the Tor software.

Tor has **extensive documentation**, and a very active community. If all else fails, you can directly email one of the developers at help@rt.torproject.org. Please bear in mind that Tor is not commercial software. So, while there is an active and helpful community, everyone is working for free, for the good of privacy and anonymity. As such, it might take a little while for them to respond to something viewed (to them, at least) as non-critical. Alternatively, the **.onions** subreddit has some helpful individuals. The same goes for **TOR**.

9. The Future of Tor

Tor remains incredibly **important to privacy and anonymity for regular internet users**, like you and I. The number of Tor users has expanded significantly throughout the last few years. Continued speculation and revelations regarding invasive surveillance practices by governments and corporations alike swell the Tor network. Moreover, the reaction to intrusive surveillance and escalating use of Tor illustrates that the service is for much, much more than the drug trade and dissident communications. It seems extremely likely that the Tor network will continue to grow.

But that doesn't mean Tor is clean sailing. For the same reasons as I've just listed, the service is the recipient of ceaseless attack. The same institutions that helped bring Tor to life — particularly the U.S. government — understand the dangers of privacy. In particular, encrypted services are on the chopping block, with many governments around the globe seeking special backdoors into encrypted services. It doesn't take a genius to workout that a backdoor for one person will never stay that way.

Indeed, in 2017, hacking group named The Shadow Brokers "liberated" **a number of extremely powerful NSA hacking tools** and previously unrealized zero-day exploits. They initially put their trove up for sale, asking for hundreds of millions of dollars worth of Bitcoin. Nobody stumped up the astronomical figure, so The Shadow Brokers did the next best thing: released the entire repository, for free.

Edward Snowden commented that the "Leak of Top Secret NSA tools reveals it's nowhere near the full library." Still, the damage was plain to see: the **WannaCryptor ransomware that surged around the globe** was a direct result of the exploits making their way into the wild. What is clear is that Tor is the tool needed to keep discourse open when those oppressors would have it dismantled.

In its current guise, Tor will remain an extraordinarily important mouthpiece against **all** regimes for decades to come.