The Essential Guide To

Tor Browsing

Includes a start up guide to installing and using Tor
Learn how to use VPN, Blockchain, Bitcoin and more.

Stay Anonymous and Safely Surf the Net like a Cyber Hacker

BRIAN BLADEN

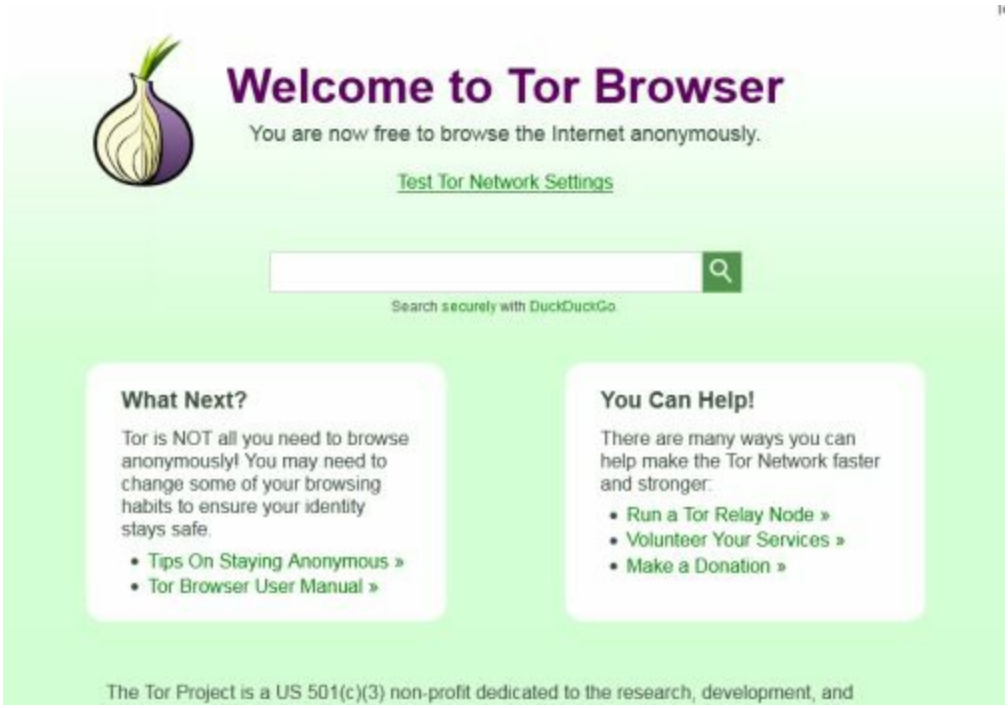
Tor Browsing

Stay Anonymous and Safely Surf the Net like a Cyber Hacker

Table of Contents

Introduction

So, what is Tor? Tor is a browser that provides anonymity by hiding your identity as you surf the web. You can browse the web, share content and engage with online users whilst remaining anonymous. Tor is an acronym for The Onion Router and was created in the US during the mid-Nineties. Tor will encrypt any data sent from your computer so that nobody can see where you are from or who you are. Tor takes its 'Onion' name from the fact encryption is built from layers. Data sent from your computer is sent through a series of 'nodes' or 'relays' (other peoples' computers) run by millions of volunteers throughout the world, building up the layers of encryption. Hence, like building the layers of an onion. Tor will hide your IP address and give you a new one every time you send or receive data. It is nearly impossible for someone to know where the data originated.



The easiest way to use Tor is by using its dedicated browser (you can download it from www.torproject.org) which is compatible with Windows, MacOS and Linux (choose the right download). The Tor browser has been designed and based on the Firefox browser but disables many of the plugins that can compromise privacy and security whilst surfing the net. Your anti-virus software and firewall may need to be re-configured in order to be able

to access the Tor network. You can also use the Tor app for an Android phone, the app is called Orbit and there is also an operating system called Tails pre-configured for Tor.

Tor is a popular browser used by police, military and government organisations across the globe. You have medical researchers, human-rights campaigners, whistle-blowers, journalists and even terrorists using the browser. All have the common requirement and that is guarding their privacy, communication and information from prying eyes. By using Tor you can choose who you associate with. There are millions of Tor users; Facebook's Tor-only version of the site is proving very popular with more than a million visitors every month.

Tor is completely legal software and was not intended for illegal activity. It is the users of Tor that can abuse its power to carry out illegal trading and crime. The same could be said of any web service – the users commit the actions. There are way more legitimate users than there are criminals and there is nothing wrong in guarding your privacy. You don't have to be too concerned with safety as Tor does not give out a directory of dark web sites. You won't stumble on illegal or disturbing content unless you have the known web address with the .onion domain.

Tor is designed to protect the personal privacy of a user by giving them the freedom to conduct confidential communication and avoid monitoring from traffic analysis and network surveillance. It was not designed with criminal activity in mind.

The History of Tor

‘The Onion Router’ (TOR) was developed in the mid-Nineties by the United States Naval Laboratory. Employees Paul Syverson, Michael G. Reed and David Goldschlag decided to develop software with the purpose of protecting U.S. intelligence communications through the net. The router was then further developed by an agency called DARPA in 1997.

TOR was patented in 2000 by the US Patent and Trademark Office after several years of research and testing.

Paul Syverson, along with Roger Dingledine and Nick Matthewson, developed the alpha version of Tor, calling it the TOR project in September 2002 and was released publicly later that year. In 2006, Dingledine and Mathewson, along with five others, founded The Tor Project responsible for maintaining TOR, based in Massachusetts. Having had several sponsors to fund the ongoing maintenance of TOR, the U.S. Government became the major source of funding. TOR also became a non-profit organisation with the obligation to disclose its finances.

Tor has developed a bad reputation with the Press over the last decade with its strong links to the Dark Web. Black markets have opened and then been shut down by law enforcement countless times, only for another market to

open to replace the last. However, Tor has proven to have some extremely effective uses:

- Citizens of countries with extreme censorship can enjoy private communication on taboo topics
- Sensitive and personal information can be accessed with privacy
- Whistle-blowers and journalists can keep confidential information a secret
- Classified information can be handled by Governments
- Parents who want to protect children from sex offenders

As you can see from that list Tor is not all about criminals trading in illegal products and services. The first major crime using Tor was uncovered in 2007 by a Swedish programmer who discovered illegal surveillance of government data using the browser.

For all its bad reputation, Tor has received recognition for its abilities. Tor was honoured with the Award for Projects of Social Benefit. The browser received the award for helping 36 million users remain anonymous over the net and assisting civil movements in Iran and Egypt.

Tor will always attract criminals and law enforcement agencies will continue to infiltrate and close down markets. In recent years, ‘The Farmer’s Market’, ‘Silk Road’ and ‘Alpha Bay’ are examples of major markets that have been infiltrated by agencies such as the FBI, and closed down.

The Tools you need

You will need a PC, Mac or Laptop with Windows, Linux or MacOS running as your operating system. You will need to select the correct download file for the operating system you use.

You will require a fast speed broadband connection for your browser to run effectively. Tor will operate a little slower than other browsers as it takes longer to communicate through the relays.

We will go into the extras you need to use along with Tor in more detail later, but the essentials include a Virtual Private Network (VPN), anonymous or temporary email, bitcoin wallets and a fake name generator. Tor on its own won't give you complete anonymity but with the extras I have just mentioned you will have maximum security. You also need to make sure your security is well maintained such as strong passwords for accounts and files, regular testing of firewalls and up-to-date effective security software. McAfee, Norton, Kaspersky, AVG, Bitdefender and Webroot are all major internet security suite providers. This is the first line of defence against hackers and a must before using any kind of browser for web surfing.

You should also look at your social media networks like Facebook and Twitter. Are your passwords strong and secure? Is confidential information like date of birth kept private? Social engineering is a common technique used by cyber criminals. It is often the human element that is the weakness when exposing personal data. Social media sites are a huge supply of personal information to criminals. Tor can be used to access sites like Facebook who have a Tor-dedicated version of their site increasing security and privacy.

The Importance of Encryption

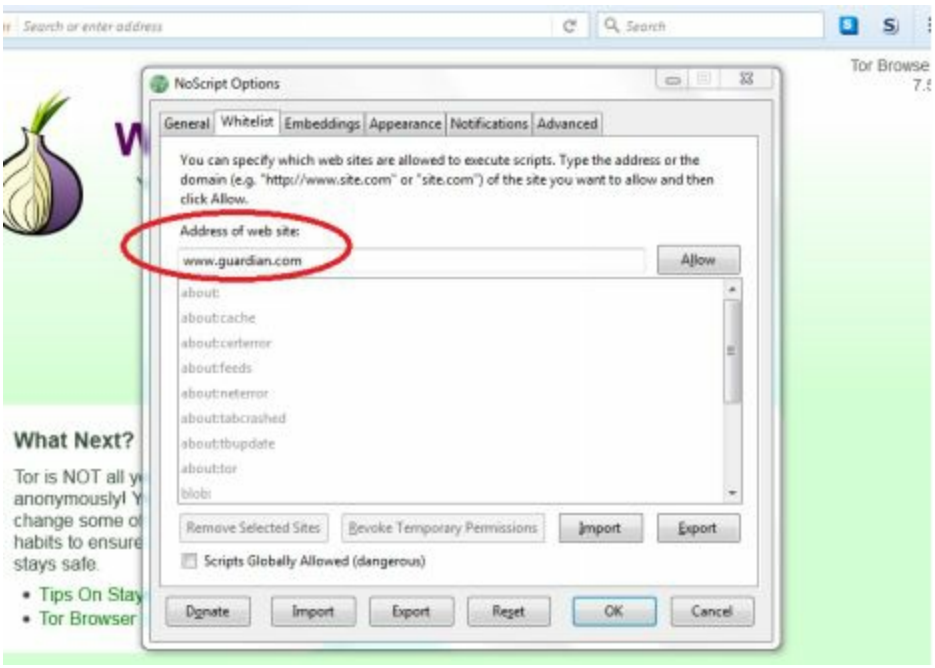
Encryption is the ability to change information in such a way that it is unreadable to anyone except those with special knowledge (or software) that allows them to change the information back to its original form. Encryption is important if you want to protect your data and don't want unauthorised users to have access to it. Encryption can securely protect folders with sensitive information such as emails, credit card numbers, accounts and other sensitive information. This has been a practise used for a long time by military and government organisations. Encryption can be used for data in 'rest' where it is stored on computers and storage devices, and also in 'transit' where data is transferred through networks (internet), mobile phones and Bluetooth devices. The common problem for data in transit is the interception of the data and eavesdropping of traffic by unauthorised users. Encryption is so important these days for things we take for granted such as banking online, internet shopping and buying financial products such as insurance and mortgages. Any weakness in encryption will be exploited by hackers, criminals, governments and terrorists. Encryption protects our infrastructure such as transport, communications and the national grid. Just imagine if terrorists were able to infiltrate this infrastructure they would have a field day! Technology in the encryption world is always moving forward getting more sophisticated and smarter. Unfortunately, as security organisations develop new systems today, tomorrow will see a group of cybercriminals using that same technology. Encryption is always evolving but one fact remains national security will always need strong encryption. The big weakness in cybersecurity threats is the human element and this is where software such as Tor should be utilised by individuals. If not Tor, then the individual or organisation they are working for need to deploy a different alternative of privacy software. Even using the Tor browser may not be enough as law enforcement agencies have demonstrated the ability to infiltrate and carry out surveillance as traffic passes through the network. This is an important time for the battle between security and surveillance and encryption is the trump card against cyber threats.

Getting Started with Tor

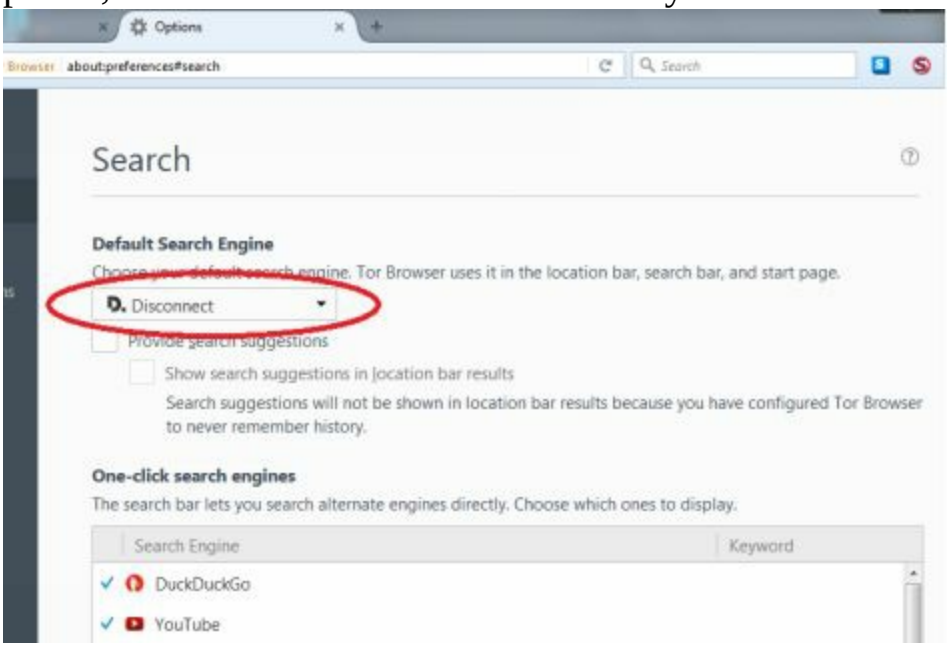
Tor is quite easy to use and the following tutorial will get you up and running with the browser. You will configure all of the important settings and use built-in tools to keep you secure and safe online.

1. Install and run Tor, and opt to connect directly to the Tor network. Click the onion icon in the top left of the address bar before you start browsing. You will be able to change the ‘circuit’ nodes through which your connection is routed.

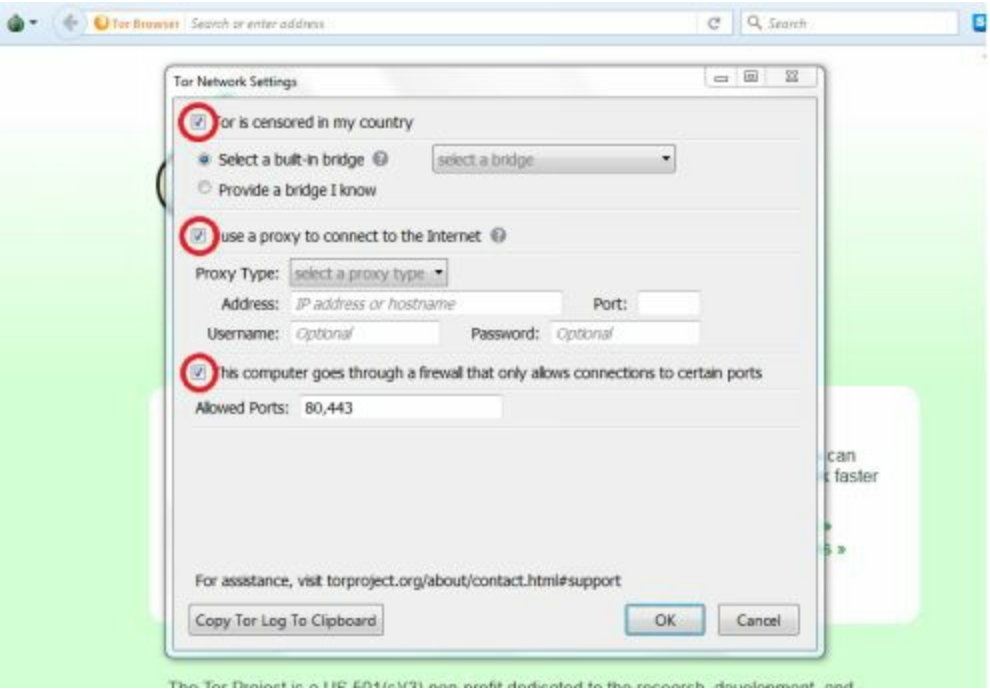
2. Click on security settings to set a security level. Tor will be set at Standard as default, this may leave you compromised. Safest will make the web look a little bare, so Safer might be the best balance between security and features.



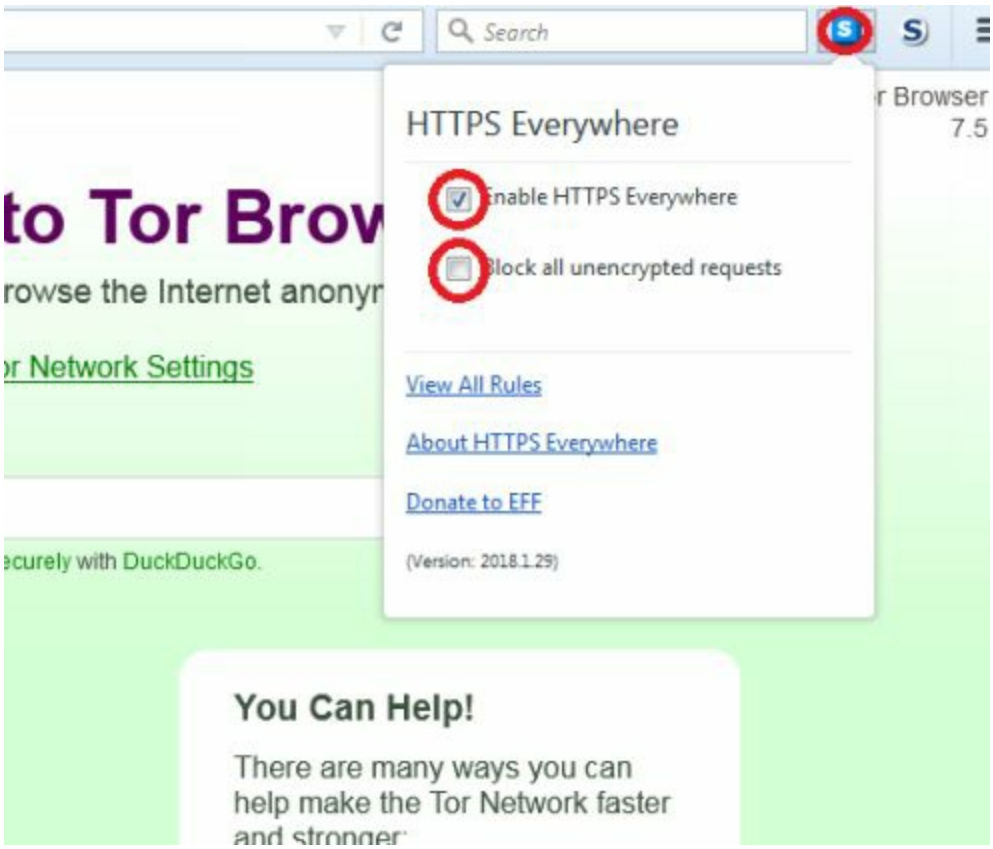
3. The NoScript add-on that has been preinstalled will block some scripts. If you choose the Safer or Safest security setting you can still run scripts on certain sites. To do this click on 'S' button, then select Options, Whitelist and enter URLs of sites you want to access.



4. To change Tor's search engine from the default DuckDuckGo, click the search icon and then click 'Change Search Settings' and then select a search engine from the drop-down menu. There are two equally private alternatives Discovery and Startpage.



5. Sometimes the '.onion' sites won't load when accessed via the address bar. If this happens select the onion icon and choose Tor Network Settings. Select the ISP option to connect using secret entry nodes 'bridges'; or computer options to connect via a proxy.



6. By selecting HTTPS Everywhere you will ensure you connect to secure and encrypted versions of sites. To select this click the top-right menu button and pick HTTPS Everywhere and ‘Block all unencrypted requests’. You can also select Choose Counter to see how well this option is doing.

Tor Extras for Safe Surfing and Purchasing

Tor will require other software in order to ensure complete anonymity when surfing the internet. Just using Tor on its own is not enough and you could still be vulnerable. The following extras I recommend are:

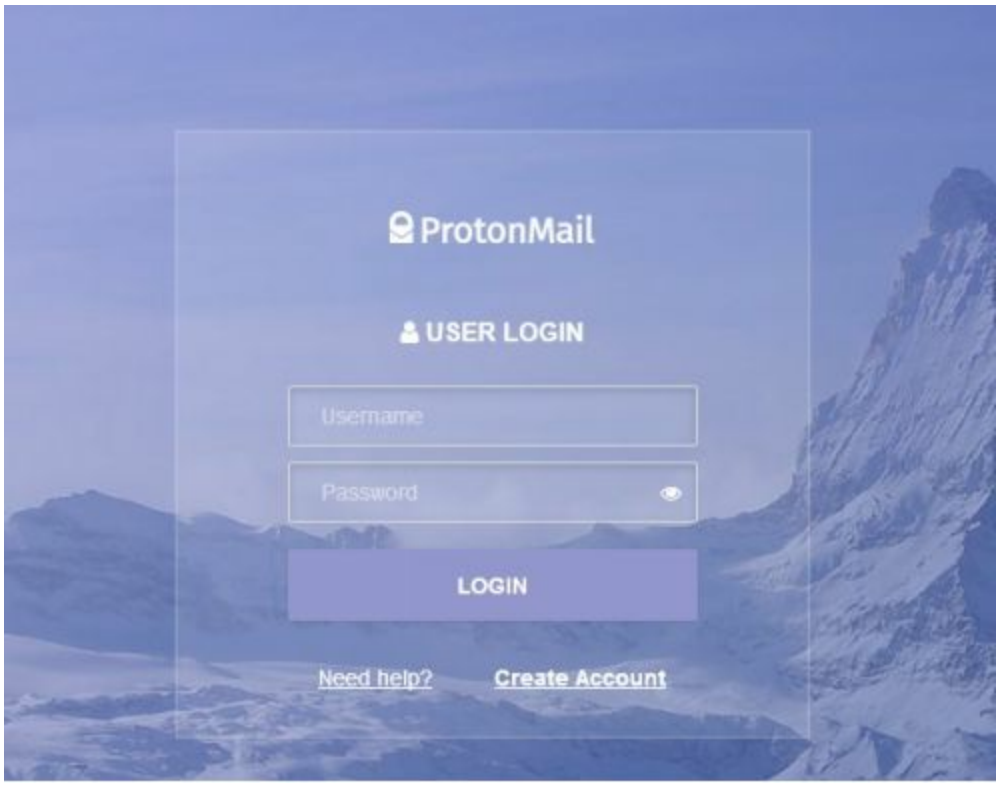
VPN

A virtual private network (VPN) can offer extra encryption to your surfing privacy using encrypted proxy connections like Tor. It will guard your IP address from the Tor entry node and your Internet Service provider will not know what you are doing on the net. If you want complete anonymity then using a VPN along with your Tor browser is a good start. Using a VPN is one of the best ways you can protect your privacy. You can purchase VPNs with fully-enabled features such as multiple IP addresses and locations to choose from. You can also download free versions that will have enough features that you require to stay private but you won't have as much choice on the location of the IP address and you may have to wait in a queue to connect. ProtonVPN is an excellent free VPN tool that will secure your connection with the strongest of encryption. The free version will limit you to only three countries of choice and connection speed s is slow but you can upgrade to paid plans that will give you more features and privacy. Windscribe is another excellent VPN but the free version will limit the data usage to 10GB per month.

Anonymous Email Services

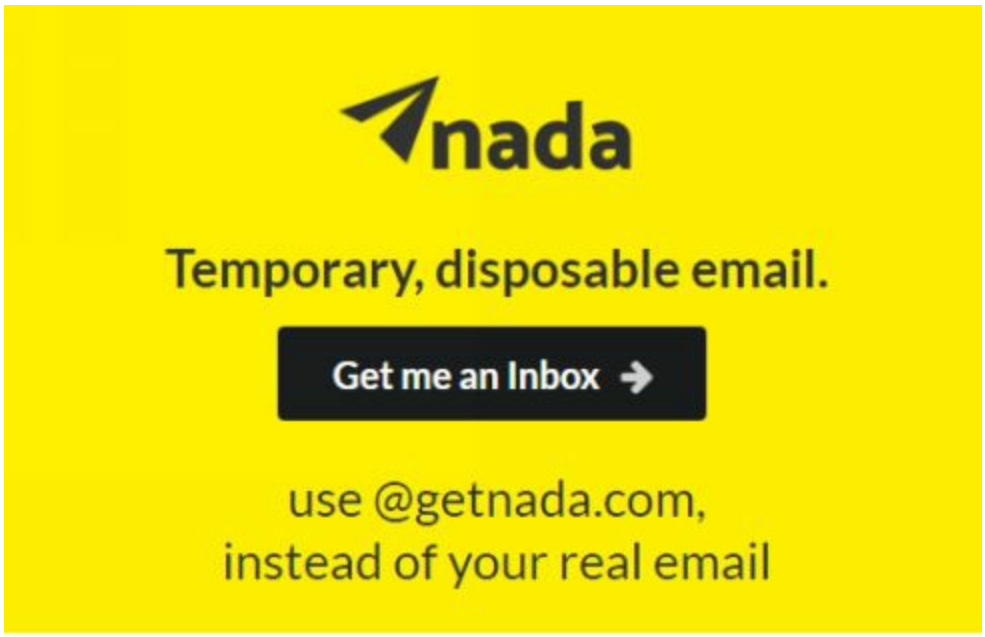
Messages won't be encrypted using a normal messaging service and anyone

intercepting them will know your name and real address. Using a Tor-enabled email service such as ProtonMail will provide total anonymity and privacy. ProtonMail, launched by the CERN research facility in 2013, is an end-to-end encrypted email provider. ProtonMail introduced a hidden service for Tor combating against censorship and surveillance. There is a free version with limited storage and messaging or you can upgrade to a paid plan for advanced features. Bitmessage is a desktop application that you can use for free that lets you send and receive encrypted messages using Tor.



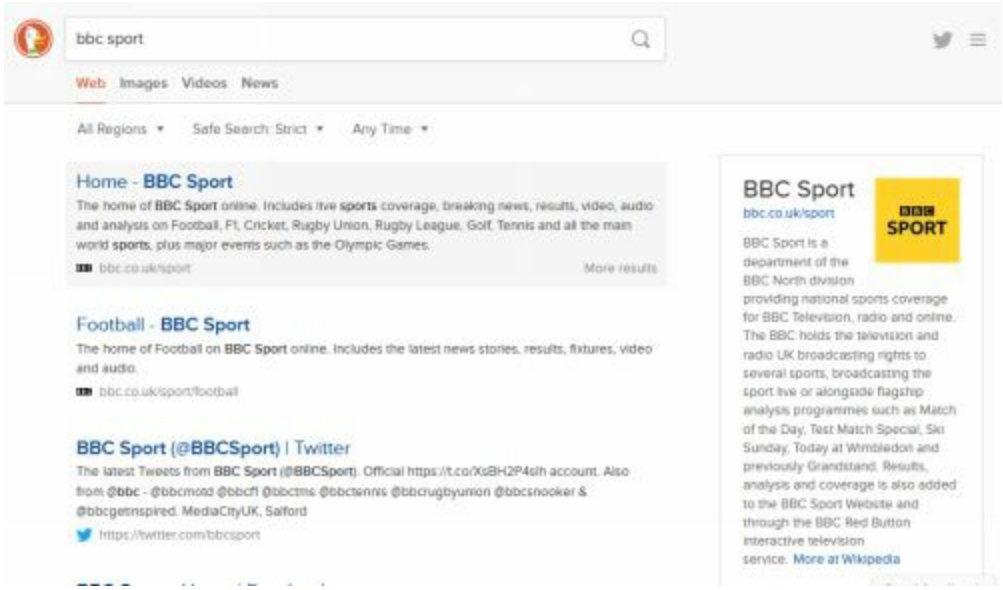
Disposable Email Address

Should you use your own email address then you are defeating the object of staying anonymous. Whilst you are browsing anonymously surveillance may be able to see the real email address you have entered. It is best practice to use a disposable email service to create a temporary email address for site registrations and keep your Tor persona separate from your real web information. Nada is good email provider as is Fake Name Generator that can provide you with a temporary email address.



Cryptocurrency Wallet
If you intend to use the Tor browser to buy and sell things then you are going to need cryptocurrency such as Bitcoin. Using a wallet can provide you with a safe account to store your currency and have access to useful idata such as the current market price. Blockchain is a popular Bitcoin wallet and it has a HTTPS certificate (most onion sites do not have this) for added security for your savings. A good alternative is Green Address which has excellent security features and instant confirmation of transactions.

DuckDuckGo
It may be the Tor's default search engine but it is worth mentioning what it does. DuckDuckGo will allow you to search the web without being spied on, taking advantage of the anonymity of Tor. It also has a useful feature where you can use abbreviated commands to search sites, such as !w for Wikipedia followed by a search topic. An alternative search engine that won't compromise your privacy is Startpage.



Hiding Tor from your ISP

Many Tor users are worried that their internet service provider (ISP) will know that they are using Tor. It is possible for ISPs to be able to detect when you are using Tor and could potentially notify law enforcement agencies. There are several methods you can use to hide Tor from your ISP and some of them are technical so you may need some assistance.

Bridges

Tor bridges, or sometimes known as Tor bridge relays, are alternative entry points to the Tor network. This will make it harder for the ISP to know when your system has entered the network, but not impossible. The Tor Project website has bridges available for you to use and configure with your browser. I recommend visiting a few sites that I have listed at the end of this guide that can assist you in using bridges.

Pluggable Transports

ISPs have found ways to block Tor even when using bridges. Censors used with ISPs can peek at network traffic and detect Tor; thus blocking the flow of traffic. Tor has introduced pluggable transports, also known as obfuscated bridges, which can circumvent the censorship. This is quite a new technology that Tor is implementing. The technology will attempt to transform your traffic into innocent looking traffic to the ISP and censors. The definition of obfuscating is to hide the intended meaning of communication making it hard to interpret and ambiguous. The plugins will basically use a protocol to transform your traffic into random pockets of data. This technology will certainly guard against your ISP; although law enforcement may be able to get a sniff that you are using Tor at the initial engagement between computer and the obfuscated bridge. To obtain an obfuscated bridge, or pluggable transport, you will have to email Tor as they are not easy to get.

Flash Proxy

The Tor browser has the ‘flash proxy’ built in through Javascript and WebSockets that can help censored internet users. Tor bridge relays can be blocked even though only a few IP addresses are handed out at a time. The flash proxy will create many IP addresses that censorship will not be able to keep pace and block them. The flash proxy will not increase bridges at static

addresses; rather they create a large and ever changing pool of addresses. The tor client will contact the flash proxy facilitator to communicate that it wants a connection. The flash proxy facilitator will keep track of clients and proxies and match them up to one another. The more people use Tor and become bridges the more options the flash proxy has, which help to prevent surveillance keeping track of the connections.

VPN

VPN is the easiest method to use and can be used with Tor to boost your privacy. The downsides of using VPN is that the provider can see what you are doing and can potentially report you and the speed of your connection, whilst secure, will be slow. It is best to connect to your VPN first selecting the IP address and location you desire before connecting to the Tor browser. If you choose to connect to Tor first then you will need to configure the VPN so that the browser works with the VPN and there are not many VPN providers that can do that (AirVPN being one of the few).

Tor Tips – the do’s and don’ts

This section explains what you should do and what you should not do with your Tor browser in order to stay anonymous and safe. Tor was developed through funding from the US Government and has been an effective tool for investigative journalists and whistle-blowers who wish to keep their contacts and information private. Today, Tor is used by normal civilians guarding their privacy and criminals looking to trade on the dark web. Below are explanations of how to make the most of the Tor network and how to avoid pitfalls too.

Do update your Tor browser as soon as an update notification pops up on the browser. Although Tor is more secure than Chrome or Firefox browsers it does not mean it is impervious to a hacker on the attack. Tor addresses threats and vulnerabilities, so it is essential that you keep the Tor browser up to date.

Do not maximise the Tor window because maximising allows websites to determine the size of your monitor. This on its own may not sound worrying but if it is combined with other information websites may be able to identify you.

Do use a Virtual Private Network (VPN) alongside the Tor browser. Tor only protects traffic routed through the browser it is not a VPN. You can boost your security and privacy by using the VPN in conjunction with Tor. The VPN will ensure all your data is encrypted and no logs are kept of your browsing activity.

Do not use Tor for torrenting to download and upload files. Tor may seem like a perfect privacy tool but using software such as BitTorrent and other peer-to-peer networks will affect your anonymity. Your real IP address will be sent to the torrent service and other 'peers'. They will then be able to identify you and view the data you are sharing. File-sharing is not encouraged

by Tor and exit nodes are configured to prevent torrent traffic.

Do create a new identity because some websites will try to track you even while using Tor. Tor will usually warn you when a site is trying to do this and gives you the option to choose a new identity by clicking on the onion icon.

Do not share your real email address, which is an obvious way of giving your identity away on the Tor network. Use a disposable email address service such as Fake Name Generator or MailDrop. You can use these services for temporary addresses when registering on sites.

Do not search the web using Google in Tor as they do not respect your privacy. By doing this you are defeating the object and giving away your anonymity. Google will track your browsing and make it difficult to use its services due to your 'suspect' manner of connecting. Sign-ins will require CAPTCHAs that ask you to prove you are not a robot, which is very irritating.

Do think about running a Tor relay to help the browser remain anonymous. The ever expanding community of Tor users are relied upon to provide the relays that create circuits. These circuits keep the browser anonymous. However, if you intend to run a relay you will need a Linux computer running Debian. If you operate with Windows then you will need to run a virtual machine with Linux and set up the relay from it. You should consider running a 'middle relay' rather than an 'exit relay'. Middle relays do not show your IP address as the source of traffic. An exit relay will and if anything illegal or malicious is carried out by another user then your IP address can be identified by the source. You could be looking at legal action against you.

Do use Tor for anonymous email because your usual email services will not encrypt your messages. Tor on its own will only disguise where you are, so you will need a Tor-enabled email service to run on the browser. Most

services have been closed down by law enforcement agencies but consider using ProtonMail. ProtonMail is an end-to-end encrypted email provider. The email provider introduced a Tor hidden service specifically to combat censorship and surveillance of users. A free account will limit your storage space and the number of messages you send per day.

Do not use too many browser add-ons as it will slow it down and compromise your privacy. Tor comes with the best add-ons already installed - NoSript and HTTPS - which is all you really need to stay anonymous.

Do report any illegal activity, especially if it involves child pornography. You can submit an anonymous report to the Internet Watch Foundation (IWF, report.iwf.org.uk). You can also report to Crimestoppers (Failing to do this could land you in serious trouble if you have stumbled on something deeply unpleasant.

Anonymity against the Government

Governments spy on individuals and companies to prevent crime and terrorist activities. Governments are always passing new laws to increase surveillance giving them greater powers on information they can access. There are some countries like Saudi Arabia that are constantly monitoring people's activity over the net with an oppressive regime. Government bodies in the UK including GCHQ and the Home Office now have the power to force communications companies to keep records of all the websites you visit and the messaging services used over the last 12 months. Government agencies can also hack into your phones, computers and networks and collect and retain confidential data. There are controls on how they use the information but they do not require a warrant, so it is easy for them to access information if they so wish. Encryption is the best way to avoid surveillance so use your VPN to guard your online communications.

You haven't just got to worry about the government hacking into your important data, cyber criminals are another problem. Cyber criminals are after your confidential information for their own financial benefit. Cyber criminals will use a range of techniques to get hold of your personal data in order to use for financial fraud and identity theft. Methods include phishing emails, malware and social engineering. Keylogging is another technique used by criminals to watch everything you type including passwords and personal information such as credit card details. They will use malware to infiltrate your computer enabling them to spy on you to steal the sensitive data. To stop this threat you should not open any suspicious emails or use software from an unknown source. Your anti-virus software should detect whether there any processes recording your key strokes.

Advertisers, internet service providers, search engines and social networks are all spying on you when you surf the net. Advertisers use cookies to track which websites you have visited that is why you will see adverts that are related to something you have looked at. Your ISP can see all of the websites that you have visited and information you have sent via messaging. They can keep records of your activity for a long time and share this with government agencies and the police. Search engines will make a log of every single

search you make so they can determine your interests. This in turn helps them to offer better search results and relevant content. The information can also be organised by your location and sites previously visited. Social networks like Facebook and Twitter will aim to build profiles on their users so they can tailor advertising. Even just clicking the ‘like’ button is helping the social network understand the sort of posts that you want to see. Tor will help guard against these privacy invaders by making it difficult to track your website visits and blocking cookies through the browser.

As you can see from reading this chapter there are a lot of prying eyes that you need to protect your privacy from. Criminals are probably the biggest worry and the techniques used for cyber security (including the use of Tor) should be focused on blocking cyber hackers.

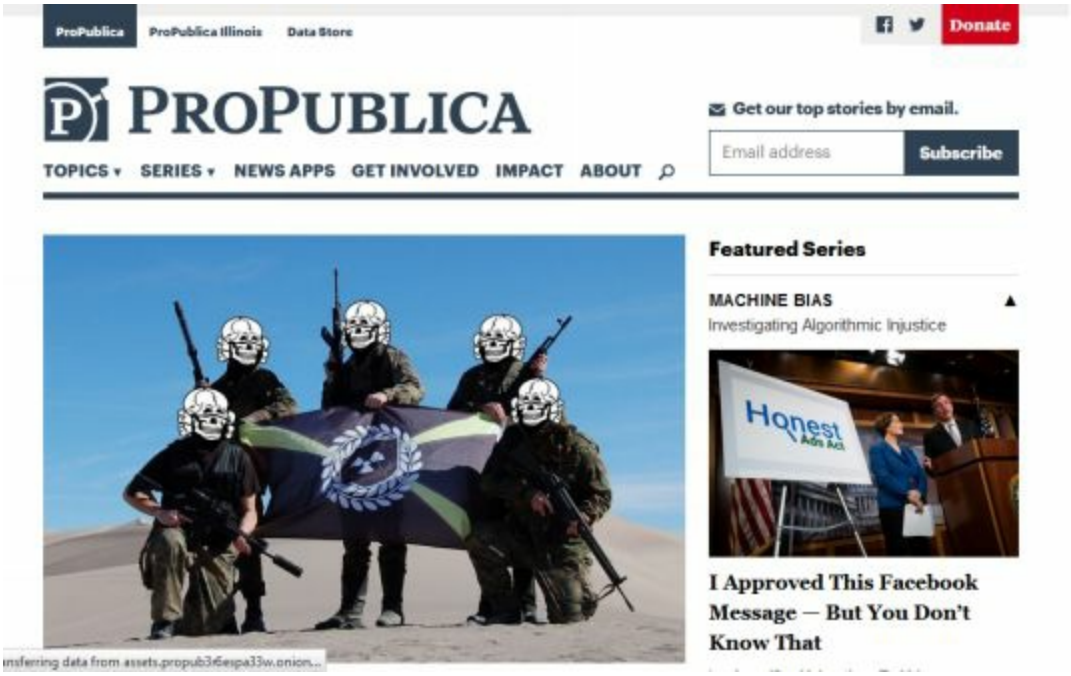
Resources

Interesting Dark Web sites – that are perfectly legal!

The Dark Web does not just consist of illegal activity; there are many useful sites that are actually legal and informative.

Facebook – www.facebookcorewwwi.onion
The social media network provides a Tor version that is a reliable and secure method of communication for people concerned about surveillance.

ProPublica – www.propub3r6espa33w.onion
ProPublic is a non-profit website that aims to expose a government that has abused its power and betrayed public trust. It is a great site for investigative journalism and allows people in internet-censored countries to read the content through the safety of Tor, without punishment.



Intel Exchange – rrcc5uuudhh4oz3c.onion
This is a must for anyone who is interested in conspiracy theories, cover-ups and leaked documents. The exchange is one of the safest places to view and

share information with some amusing threads.

WikiLeaks – wlupld3ptjvsgwqw.onion
A renowned site mostly because of the recent press coverage it has received resulting in WikiLeaks founder, Julian Assange, losing a lot of goodwill. The site still holds a lot of acclaim and has important sources of uncensored political information. If there is anything sinister going on in politics this site sets out to uncover the truth, even at the expense of a court case. You can access the site on any browser but documents have to be submitted through Tor. Files will be encrypted during the upload.

Flashlight – kxojy6ygju4h6lwn.onion
This site gathers information and news about online privacy, bitcoins and Tor-related projects. The site is a constantly updated news feed along with a forum for discussion.

Tor Project

Use this site to download Tor and get support
https://www.torproject.org/

Virtual Private Networks

ProtonVPN - https://protonvpn.com/
Windscribe - https://windscribe.com/

Anonymous Email Providers

ProtonMail - https://protonmail.com/ or protonirockerxow.onion for Tor
Bitmessage - https://bitmessage.org/ or bitmailendavbec.onion for Tor

Bitcoin Wallets

Use one of these wallets to securely store your cryptocurrency

Green Address - https://greenaddress.it/en/
Blockchain - https://www.blockchain.com/ or blockchainbdgpzk.onion for Tor

Disposable Email Service

Nada - https://getnada.com/
Fake Name Generator - https://www.fakenamegenerator.com/

Magazines and Websites

WebUser – UK magazine published fortnightly with excellent tips on staying anonymous online.

DeepDotWeb - https://www.deepdotweb.com/
Lots of interesting articles and new stories linked with the Dark Web