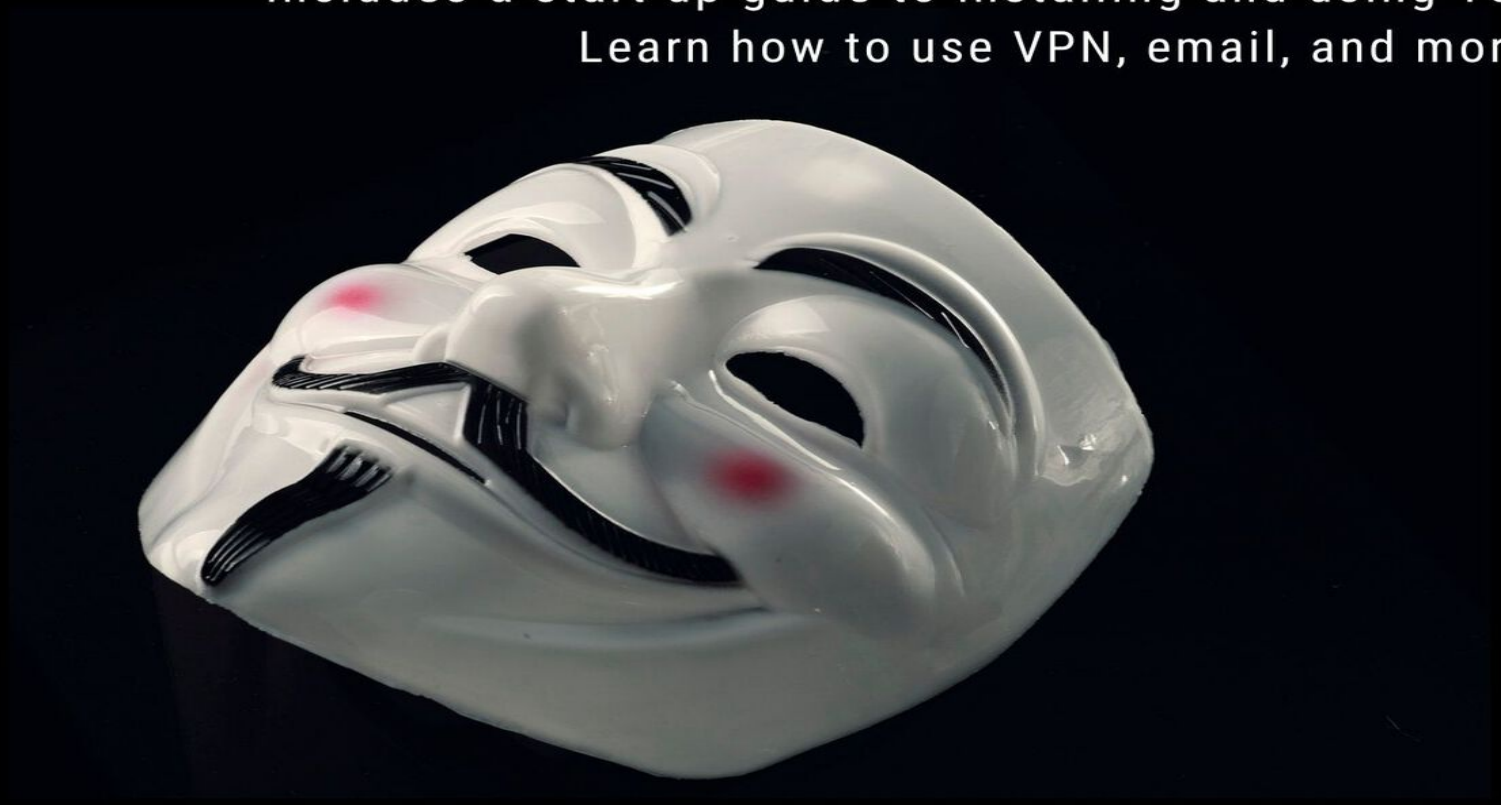
The Essential Guide To

Tor Browsing

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



Stay Anonymous and Safely Surf the Net like a Cyber Hacker

BRIAN BLADEN

2ND EDITION

Tor Browsing

Stay Anonymous and Safely Surf the Net like a Cyber Hacker

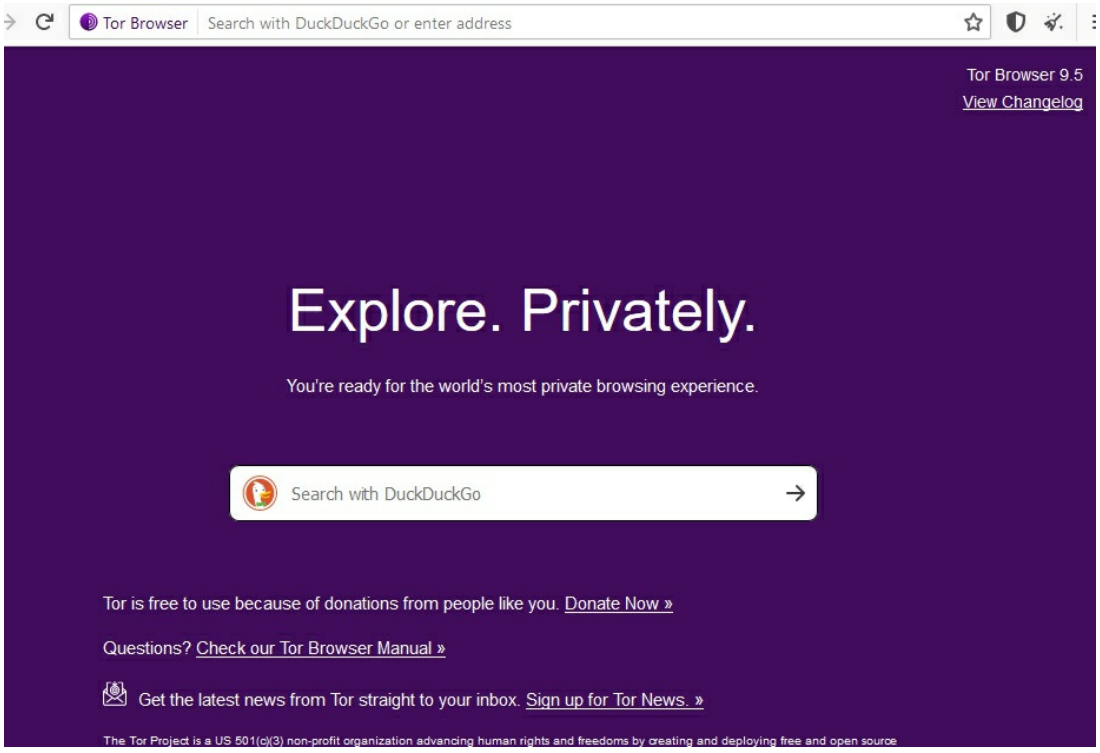
Disclaimer

This eBook was written for the purpose of teaching people how to stay secure and anonymous in the digital world. It is a book written for people who are in difficult situations such as whistle-blowing journalists, activists, somebody being hunted or persecuted by their government, investigators and researchers, or a person who is threatened by someone else. The book details techniques on staying digitally private and some of these techniques are the same ones criminals may use as well. We do not condone the actions of criminals and this book is not intended for criminal activity. How you use the information in this book is your choice and we cannot be held accountable for your actions.

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.

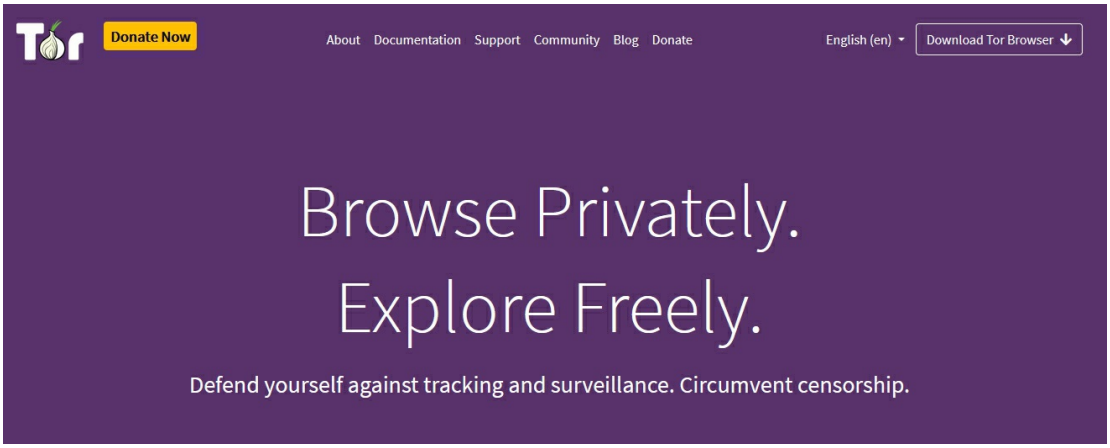
Tor is designed to protect the personal privacy of a user by giving them the freedom to conduct confidential communication and avoid monitoring from traffic analysis and network surveillance. It was not designed with criminal activity in mind.

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.