TOR BROWSER

Secrets of the Deep Web, How to Stay Anonymous Online, and Surf the Web Like a Hacker

COOPER ALVIN

Tor Browser

Secrets of the Deep Web, How to Stay Anonymous Online, and Surf the Web Like a Hacker

Table of Contents

Introduction

A few words about the book, *"Tor Browser."*

This book contains information vital for those who wish to surf the Internet anonymously.

Before you read this book, you must ask yourself the following questions:

- How much do you know about the Tor Browser?

- How much do you know about the Dark Web and the Deep Web?

- Are you currently anonymous online?

This book sets about informing you of these aspects in as simple a fashion as possible.

This book does not confuse the reader with jargon and acronyms from computer science. It explains what each acronym is, and what it is about.

It is authored for an intelligent layperson. You will learn a lot from it. Its contents should make you a bit worried.

It will tell you about computer basics, general online safety, the Tor Browser, the Dark Web and the Deep Web.

It tells you what to do if you want to surf the web like a hacker.

There are so many things this book can do, if you only take the chance to read through it.

Now start reading!

Background

What is a computer?

I am not going to delve too deeply into this topic as it is very complex and has many layers. It is enough for you to know a computer is an electronic device, which does intricate things with data (information). Whilst a simple definition may give you a basic knowledge of what a computer does, it does not even hint at the extent to which computers and electronic devices affect our everyday lives. They are everywhere we turn, even at the ATM where we delve into your bank account. To a certain degree, we tend to believe that all these different interactions are carried out safely and with our best interests at heart.

One of the largest and easiest to identify ways in which computers have brought change into our lives, is by examining the impact on the workplace. Prior to computerization paperwork and information sharing, were the task of many different individuals constantly tracking information. It is used to check figures and filing all the paperwork this would generate. Now, of course, a computer can store vast amounts of information that is readily available to virtually anyone at the click of a mouse. It is that easy to access. File cabinets and libraries are a thing of the past. Jobs that would previously take many people a number of work hours to complete, can be completed in a matter of seconds.

Similarly, with computers information and files can be shared worldwide with a click of a button leading to a greater marketplace and a less structured working day.

Factories are another good example of the effects that computers have had on the workplace with computers replacing employees to do most aspects of the assembly line. There are many people that do not believe a computer can do work better than a computer, but in this day and age, a computer can process more data quicker than a person can. It is an advantage most, if not all, factories have converted to.

Computer languages

Like computers, computer languages are a huge and complex field, which you really don't have to know too much about, except knowing a computer

language called JavaScript. With this language, many of the things you do with keystrokes, mouse clicks, etc. If this were all that JavaScript did there would be no problem. However, like so many things that people create, there is a dark side. A dark side many do not know is there to begin with.

By using JavaScript, hackers, businesses, and others are able to get access to things you would prefer that stayed hidden. In some cases, you may think they are hidden away from the world. However, that is not the case. Everyone can get any type of information that is posted online, even your most private of information. I will occasionally be talking about JavaScript, so do not be surprised when I do. I will refrain from any discussion about programming in this book or mention any other language as it can easily confuse those that so not have it in their repertoire.

What is the definition of Server?

A strict definition of a *server,* is that it is a computer program that delivers stuff to other computers. It can range from the simplest of forms, to your entire life story. Often the computer that the server program works in is called a server. It is basically speaking of how computers join together so they *talk* to one another. In other words, this can be called *networking* the computers as well. A *network* is a family of interconnected computers all striving for the same output as the original. Servers can provide various services, which include sharing data amongst multiple clients. Servers like this one can send varied content toward each client. Clients can also utilize multiple servers at the same time. Typical servers are mail servers, print servers, app servers, database servers, game servers and file servers. What that appropriately means, is that a computer or a computer program can manage to access a centralized resource or service in any particular network that it deems fit.

What is the definition of the Internet?

The internet arose from an advanced research project established in the 1960's by the US department of defense. In order to do this, they collaborated in research between military and government laboratories. It is called, Arpanet, and at the time it gradually led to other connections with US universities and other US institutions for its extended use. In doing so, this resulted in a growth that was so beyond expectation it was mind

crippling even to ponder about. This system also led to the development of what we know today as the Internet. It is the system we scour every minute, without truly knowing what went into its creation. Few people know the advanced coding it took for any one person to make this dream a reality.

The explosive world growth that we now know today was facilitated by the development of the hypertext-based technology, that's called the World Wide Web,

You may see on the navigation panel, WWW, which is otherwise known as the World Wide Web to most of us, provides us with and easier way to search and navigate tools. It is a means to display text and graphics with a general ease of access and use that means of your new capable knowledge so that you can all make the most of your time spent online.

The term is often mistaken as a reference to the internet itself, but the internet predates the WWW significantly. In the early days, the first web page created is now lost, however, if you search far enough there is a copy of a page sent. In 1991 by the inventor of the WWW, Tim Berners-Lee to a Paul Jones in North Carolina, you can search it and find that it is the oldest web page in existence. It was taken offline for some time, but soon it was put back online in 2014. It gives you helpful links that help people navigate what was then a very small worldwide web. You may not think this is useful, but it is. To know the way, they navigated the system before it grew to be as huge as it is today, is phenomenal.

The Internet is a global system of interconnected computer networks. The networks in the Internet exchange data through a complex process called *packet switching*. There are protocols (rules) that make this happen. It may be hard to divest the knowledge, but once you get the hang of it, you will be able to properly decode how the internet was invented and why it was invented.

Another interesting fact about the internet, is that nobody actually owns it. It may have a creator; someone that took their time to properly put the network together. However, there is no one that truly owns the internet and all it entails. Just let that little tidbit of information sink in. Possibly the greatest influence on society, that this world has ever seen in recent memory, has no owner. No one to claim they are over it. Several various

organizations worldwide are responsible for its development and ability to function, but none of them are able to fully take credit for its discovery. The high-speed fiber optic cables that are responsible for the bulk of the internet's data transportation are owned by phone companies in their respective countries, but that is as far as it goes when saying someone owns the internet. They do not, they simply own the things it takes to keep the internet up and running.

In summary, the Internet is a system of networks containing millions of all sorts of smaller domestic, commercial, governmental, etc. networks with all the services and information such as SMS, email, file transfer and all other parts of the World Wide Web (WWW).

How does the internet impact our lives on a daily basis even without us knowing it??

The IOT, which is a simple term meaning for the Internet of things; it may be a simple term, but it is a concept that many people find hard to embrace even in todays time. Many discussions are based on future impact in years to come whilst almost ignoring the many ways the Internet of things already affects our daily lives.

1. Health and exercise

Gyms of the future filled with IOT gadgets carefully monitoring every aspect of our daily health may seem to be a way off, but are they really? Don’t we already have a vast array of wearable technology already monitoring our health and fitness? From the smart watch that can track your every step, every calorie burned and monitor your heart whilst doing so (FitBit). We have all of these devices around us, but we do not really look into what all it entails; what all goes into making those gadgets possibly to work.

It not only helps you to stay in shape, but it keeps a track on other aspects of your health as it is performing its job. With revolutionary gadgets, it is now possible to monitor glucose levels with a smartphone app, which can be essential for diabetics. This way they do not have to poke themselves as many times a day to know their readings. They can simply glance at their watch, seeing what their blood sugar levels are.

The second generation I watch and Simbands also include heart rate monitors and other health trackers. In doing so, it allows doctors to monitor patients and provide the optimum care that the patient requires from afar. Just imagine the benefits that can be gained from your doctor having the ability to view your statistics on a 24-hour basis, and this is all down to a piece of technology no bigger than a watch.

They will be able to help you while you are not in their presence. They will be able to see, as it is happening, your health statistics, whether they are declining or rising. You will not have to keep a log anymore. You will not have to bring all of that information with you when you appear before your doctor. They will already have that information saved in a folder on their computers.

2. Pollution and waste management

Smart ways of dealing with the problem of pollution and waste management include: Waterbee.eu, which is a system used by farmers and other enterprises that use huge amounts of water to conserve water. They do this by monitoring the soil and if they find it is getting too much moisture, they can adjust the water usage accordingly. It is very scientific in that aspect, but it will save on a lot of time and resources once it is complete.

Also, on a more domestic level, is a device call AirQualityEgg.com, in which monitors the air quality around your home, office, and then when it gathers enough information, it analyses the data to help understand how different policies are affecting urban pollution. Pollution is our biggest downfall as a society, and to know there are websites out there that will be able to explain how much pollution is in a single area, is big. You will be able to determine for yourself if that area is worth exploring, and all of that is produced by the single click of a button.

3. Around the home

A “smart house” is often the first thought that occurs to people when discussing IOT, maybe because this is possibly the biggest personal impact that smart technological gadgets can have on an individual. Some may think it is a house, like on the movie they show on the Disney Channel. However,

that is furthest from the truth. A smart house is actually a security system that allows you to monitor your home while being online.

You may not believe it, but it is already the norm for a great number of people. That is, if you can fit it into your budget. Society thrives on technology like this. With the ability to turn off your heating and cooling, or your lights for that matter, when away from your house and then turn it on before you arrive is a great tool in energy conservation. You will find with this little gadget, that you have lower electricity bills and you are saving on resources you did not even know you were using before. Not only is IOT providing great help around the house, but it is also a helpful tool to manage the monitoring of pets and children. The sensors the company places around your home can alert you when certain doors have been opened in your home and can thus greatly aid caregivers who have had to leave the house by alerting them to potentially dangerous activities. It is also an effective tool to have against burglaries. It will let you know when an intruder has been spotted in your residence. You will be able to effectively, and safely contact the authorities and take care of the perpetrator.

Also, another plus of this, is if you have a newborn baby. You can significantly benefit from IOT with what they call, “smart baby sleepsuits.” This is a suit the mother or father can place on the infant that monitor their sleep patterns and heart rate. It can even alert you if any problems arise. If you have a newborn baby, you know how effective this little suit can be. You will not be able to continuously pack the infant around, and thus this suit will give you the specs of the newborn through digital uses.

The next item that is effective for you to obtain, is a smart refrigerator. By having a smart refrigerator in your home, you can ensure that you do not have to make a second trip to the store because you forgot something. Your refrigerator can sense when you are running low on staple foods such as butter, milk, and eggs and can add them to your online grocery lists. On most of the refrigerators, there will be a screen located on the front, telling you when you are low on these certain items. It is great when you are on the go and have to be out of the house in a hurry. You can simply glance at the front of the refrigerator, and it will tell you what you need.

You may not believe it, but even the garden can benefit from IOT. There are many products that range from a gutter cleaning robot to a remote-control system to water your lawn. You will be able to remote activate it while you are inside your home. Knowing these IOT's have it under control will guarantee that you won't have to worry about doing these chores yourself. You will be able to free up your schedule and do other things more important, like spend time with your family.

4. Transport

Now content with impacting our homes and work, IOT is also heavily featured in the future of our daily commute. Yes, it is everywhere as far as the eye can see. Already our sat-nav systems are working with real time traffic conditions, and finding alternative routes to avoid stressful driving conditions. Have you ever heard of a GPS? This is the device that uses that type of IOT, so we can efficiently and safely get to our destination. That is the reason a GPS needs to be updated every so often. Because if there are new roads and stopping mechanisms in place, it will not know about them unless it has been updated.

For the streets, traffic lights are set to be able to monitor different situations and react accordingly. For instance, in the case of an emergency vehicle approaching. Road sensors will be able to communicate directly to your car dashboard and inform your vehicle of any hazardous conditions ahead, e.g. the turn on your left in a quarter of a mile is icy so slow down to avoid danger. You may believe they are there to harm our way of live, but in fact, it is the opposite. IOT's help us out of difficult situations every day.

Your commute to work can be altered by variables such as weather, road construction and accidents on your normal route. So, by having your alarm set to detect these variables it can then adjust your alarm call to allow for the extra time needed for your journey. If that isn't enough, it can then interact with your dashboard and ensure that alternative routes are available. So, pretty much everything is synchronized to an IOT in some form or another. Just don't forget to synchronize your coffee machine to make sure you have that much-needed cup of coffee to kick start your morning.

Smartphones are set to become everyone's portal to the Internet of Things ecosystem, and more importantly, it is a complete remote control for our

lives. With the ultimate smartphone apps that are available today, your smartphone is a smart platform with which to optimize the apps that are pertinent to your life. You should use them to their full capacity. Just think of your smartphone as the ultimate Universal Remote Control. Anything you would ever need is in that phone. You can download the apps, then program them with what you want them to accomplish. It is easy and pretty straightforward.

Web Server?

A computer program which serves web pages is called a *web server*. A web server, is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form web pages for users. A direct request can lead to a response that is forwarded by their computers HTTP clients. Considerations when choosing a web server should include the security characteristics involved and its ability to work alongside other servers and operating programs. You do not want to choose a web server that is known for being glitchy, as this can lead to virus' spread on your computer. It can also reach the files stored on your computer and crash them. The web server is read by browsers, which include, but are not limited to, Firefox, Internet Explorer and Chrome, they then convert the files into text and images for your information. Choose your browser well to optimize your internet activity and it will ensure that you are getting the exact information you are requesting. As you probably already know, each browser is different. They have different commands that do a multitude of things. The main factor is, since they so closely correlate, is the become used to the browsers before doing anything else. You need to make sure you have accurate knowledge of it and what it all entails.

A program which requests web pages is also called a *web client*. Web client is another term for *browsers*. Other examples of well-known browsers are Apache, Google web server, and Safari. Yes, and even though they may be web browsers, it does not mean they can do the same thing as the others. There are programs—websites—that do not work for some of the web browsers. You must be able to read the fine print on those websites to see which browser works best for what page.

Web Pages

The definition of a *web* page is very simple. All computer files have a name which finishes with a *suffix* such as .docx, .pdf, .jpeg, etc. Web pages are files on the Internet with the suffix *.html, .com, .org, or .gov*. Browsers are what you use to access them. Such files are the most important part of the World Wide Web (WWW), which is a very important part of the Internet. You use these pages specifically to find what you are looking for. They are what bring your information to you.

HTML was first used in 1989. It was from the creation of Sir Tim Berners-Lee, who was a scientist and computer programmer at the European Laboratory for Particle Physics in Switzerland. Everyone was trying to find out how to make browsers work systematically with the web pages, and he is the only person to find out that you needed an HTML to be able to gather the information you need to find.

HTML has been developed a lot since 1989, and at the moment we use HTML 5, which is the fifth version since its creation. Readers can expect further development of HTML as new uses for HTML are discovered. Right now the HTML 5 does have a lot of perks, however, there are still times that you cannot find the information you are looking for, and that is because the coding gets lost in translation. Developers are hoping to get this matter solved, that way when you search a certain topic, you will get the desired results.

The JavaScript Computer Language

The topic of computer languages was previously discussed, and JavaScript was mentioned as being one of those computer languages. JavaScript is very important for the Internet to produce what it does. You will be told what you need to know later, but no attempt will be made to teach this powerful language to you. It is so diverse that it would take a millennium to be able to break through the outside barrier of it. It is that complex of a system.

JavaScript and Java, Are they the same?

You may have heard about the Java programming language. This is a very powerful computer language which can be used for a plethora number of things. One of its most important current uses to date, is for creating apps

for the Android Operating System, which runs billions of non-Apple devices. When you turn on your phone and search the internet, Java is operating those systems, making it able for you to do what you want to on your phone.

Java and JavaScript are completely different computer languages with only a similarity in name. Although both are not too difficult to learn, JavaScript is much easier to learn and can also be used for making apps but we will not go into this.

Chapter 1: Protocols

Earlier in this book, references were made about protocols being the means of which computers 'talk' to each other. Humans, when they converse, do not have to be too rigid in the use of language. We all will know what the other person is saying if they simply convey their message. This is not the case with computers. The means by which computers converse is electronically controlled. The exact nature of how this occurs is quite complicated.

The first stage in a computer conversation is 'handshaking.' This establishes a connection between the computers. In simple terms, this means that the computers are getting a connection between each other. Their IP addresses are synchronizing so they can make this happen. What happens after that is governed by *protocols,* which apply to the different types of Internet actions. In this case, such as email, SMS or web surfing. Information sent over the Internet usually involves the message being split into smaller packets, which are reassembled once their destination is reached. It makes it easier to get the message across to the other side. If it does not split up into multiple packets, then the message could take years to get through to the computer it is linked to.

TCP: TCP is the protocol which splits the data into packets for transmission. It makes it easier for them to be sent. Upon being sent, it breaks them up into little packets. And when it gets to the other side, being delivered to the client, it reassembles them and ensures that no packets are lost in transmission. TCP stands for Transmission Control Protocol. Its acronym is pretty self-explanatory.

IP: IP stands for Internet Protocol, which directs information to the correct address. Every computer connected to the Internet has its own address. This is of great importance when we start up discussions on safety online. IP does not connect to computers. That is one of the roles of TCP. It only manages the routes by which the packets travel. Anything done by that IP address can be seen by others if they dig deep enough. They will be able to see what you did, when you looked it up, and how you went about your

business. You can wipe the hard drive of your computer, but your IP address will continue to have that information stored on your computer.

Pop3/IMAP: One of the most valued parts of the Internet is email. Email is governed by protocols. The protocol for sending email is SMTP, which stands for Simple Mail Transfer Protocol. The protocol for receiving email is either POP3, which stands for Post Office Protocol 3 or IMAP, which stands for Interactive Mail Access Protocol. You may believe it is as simple as the click of a button, but there are many protocols that go into sending and receiving a simply email.

HTTP/ HTTPS: The World Wide Web is constructed of files with the suffix HTML. Web pages are governed by the protocol HTTP, which stands for Hypertext Transfer Protocol. If you copy and paste from the address bar of your browser, then you will inevitably see a sentence which starts HTTP:// … In some cases, more so than others, you might see HTTPS instead of HTTP. HTTPS stands for Hypertext Transfer Protocol Over Secure Socket Layer. This means that any transmission from this page is in an encrypted form and is theoretically unreadable. We will have more to say about this later.

FTP: This acronym stands for File Transfer Protocol. This will not usually affect you unless you upload material to websites using FTP programs such as FileZilla.

This completes a very brief discussion over the list of protocols you might face when using the Internet. There is far more than can be written on the topic. So much so, that it would take more than simply this chapter to explain them all. What I have provided you with are the main focal points that systematically help the Internet do what it needs to do.

Chapter 2: Are You Being Tracked Online?

Is your online activity being tracked? Could it be and you simply do not know? It is a common experience for someone to click on something on a web page that interests them: a book, a piece of clothing, a music file, etc. Once this is done, you will find ads starting to pop up in all sorts of places such as Facebook, email, Google etc.

You may find this an absolute nuisance and put in an ad blocker, which can help, but it can also create some problems for you. The reason the act of clicking on that item produced the flurry of ads was that your online activity was being tracked even though you did not realize it. There are people that set up blocks, so when a particular item is clicked, then they will know. All of their processed information, such as web pages will then begin to attack your computer.

One of the things that have been predicted is the rise of individualized prices. The fact that you paid a lot for a clothing item may be taken as a sign that you will pay a lot for other things. You may decide to buy some music and the price you are quoted will be higher than the price to someone else who is believed to be worth less.

Brick and mortar companies are also gathering information about you. If you have a loyalty card, then every time you use it when you make a purchase you will find information about that purchase is being secretly recorded. You can expect emails or other communication with information about other items, which would possibly interest you.

Another fact people don't know is that some shops track people's Wi-Fi signals and see what aisles they may browse through. This information is predominantly used within the shop to help decide on the display of merchandise. If you do not want to help the shop find out where you go, then switch your device off before you go into the shop.

The data being collected may be things you have entered yourself such as name, address and credit card details. Other information is also available to be harvested such as details about your device, the sites you frequent, your online activity and other things.

There are other ways in which tracking is being practiced. A defense giant called Raytheon has developed a piece of software called RIOT. It targets Facebook and builds a picture of a person of interest. It focuses on such things as logins, longitudes, latitudes, other details from photographs, and a number of other things which enable a pattern to be built up.

In the past, such tracking was quite difficult and so only targets of interest were tracked. Now, with the development of big data and the artificial intelligence to enable patterns to be discerned in this big data, it is sensible for mass surveillance to occur.

The idea behind this is that by finding the patterns of behavior of ordinary people, the behavior of those of interest: the criminals, child abusers, terrorists etc. will be more clearly revealed. The argument is put forward that if you have nothing to hide then you have nothing to fear and this might seem reasonable.

However, if the data trawled by software such as RIOT falls into the wrong hands then serious problems could arise for completely innocent people.

There is another technology being used by those who wish to track you online. It is totally different to the ideas of RIOT. The method is called *canvas fingerprinting*. It is based on a really clever idea, which is that individual computers have fingerprints, which are unique.

The canvas fingerprinting program gets your computer to send a picture of some text. Each computer's text is unique to that computer. This technology is actually a tracking of the device, rather than a person. However, if only one person uses the device then it is, in reality, a check on the person.

Sites ranging from YouPorn to the White House have used this technology. YouPorn claim they no longer use it. The existence of these two different technologies and others imply that you will always be tracked when you go online. It is believed that at least 5% of the top 100,000 websites use canvas fingerprinting including US and Canadian government sites.

All sorts of organizations do the tracking: social media, cell phone companies, email services, cell phone apps, search engines etc. All of these organizations are compiling records of your online activity.

This compilation may seem quite innocent, but if your information falls into the wrong hands such as a government spy organizations, the mafia or other criminal group or even a snooper, there could be disastrous consequences such as wrongful arrest, identity theft, online ransom etc.

There are ways to prevent this information from being available. It is the purpose of this book to discuss these. Various methods of online privacy will be discussed with particular attention paid to one method, which is the use of the TOR browser. We will discuss this browser thoroughly in Chapter 4. In the next chapter, we will discuss online privacy in general.

Chapter 3: How to Stay Anonymous Online

IP Address: Earlier, reference was made to the unique address that your computer has which is called the IP address. This is a unique identifier for your computer. There are two versions of this - the IPv4 and the IPv6. The number of numbers that were possible with IPv4 ran out and so the IPv6 came into existence during 2015. You don't have to know the details of these identification numbers unless you're interested. Just remember these addresses exist and are of great interest to people and organizations that wish to track you while you are online.

Mac Address: Another series of numbers, which is associated with your computer and which should be hidden or disguised is the Mac address. This identifies the network adapter, which is on your computer. It is composed of a number of pairs of numbers separated by colons. If you are interested you can Google the means by which you can find your Mac address.

In this context, Mac does not refer to a Macintosh computer. It refers to the Media Access Control address of your computer. All computers, whether they use Windows, Macintosh, iOS, Android or Linux operating systems, will have these if they connect to the Internet, which nearly all computers nowadays do. Like the IP address, the Mac address is of great interest to those who wish to track you online.

The previous chapter identified reasons for preventing others from snooping on your online activity. If a large organization with vast resources such as the CIA wants to track you, they will and you will have to be incredibly clever to avoid this. Despite this, here are a few tips for being as anonymous as possible:

1. Use private sessions when you surf the Internet. All common browsers such as Firefox, Chrome, and Safari have this ability. Be aware that such private browsing really is only of domestic use. Even in a work or school situation, the network administrator will see what you are up to on the Internet.
2. Logins: Use different passwords for different sites. This is a nuisance but it is far preferable to have a lot of passwords, and possibly a

notebook to keep them in than to have your credit card used by a hacker for making a $10,000 purchase in Manila!

3. Delete all cookies and delete them often. Cookies are tiny files that many websites place on your browser for a variety of reasons, most of which are innocent. Again, this is only of domestic use. Don't think that because you've deleted cookies that you are safe online.
4. Don't let your browser send location data. If you do not want your location known then this is a no-brainer. All major browsers have the ability to prevent them sending your location data forward.
5. Don't let Google track you. Google is a very good search engine and is used by the vast majority of Internet users. However, it is better if you prevent Google from tracking you. If you don't do this, you will be at the mercy of advertisers. Later on, we will tell you about the Epic browser which stops Google's tricks.
6. Set social media, such as Facebook, Twitter and Linked In, privacy settings to give you maximum privacy. It is frightening to discover the amount of personal data available on social media sites such as Facebook and Twitter, this is the price you pay for using a free service, try on Facebook settings downloading a copy of your Facebook data and you will see every activity you have ever done on Facebook recorded in your data history. There are similar levels of data harvesting opportunities on all social media sites and the only way to prevent this happening is by deleting your accounts completely. Even de-activating will not clear the information merely put it into hibernation should you wish to re-activate your account.
7. Use an add-on such as Privacy Badger to block trackers. Privacy Badger is a browser add-on tool that detects sites that may be trying to track your activities in an objectionable and non-consensual manner, your copy of Private Badger will keep a note of any third-party domains that are active on the websites you visit that may track you without permission by using cookies to collect a record of your online activities. Privacy Bandit will disallow content from all third-party tracker unless the third-party domain plays an important part in the make-up of the website such as embedded maps or images. In

cases such as these Privacy Badger will allow connections but will remove potentially dangerous tracking cookies.

Other add-on tools are available such as AdBlock Plus, AdBlock ultimate and Tinfoil for Facebook, it may pay off to check out the right software that fits your style of surfing.

8. Disable Java, JavaScript and all plug-ins that you do not use. Because JavaScript is so widely used on web pages, this may be impossible to do in all cases. If you go to travel sites, which often use a lot of JavaScript, be very careful.
9. Use the *Epic* browser. This is a form of Chromium, very similar to Chrome, which has many of the features endorsed before being included in the browser. It also reveals how many trackers tried to follow you each day. This browser is quickly becoming one of the most popular web browsers and is incredibly popular amongst the populations of China the US and Nigeria.

When using Epic data is automatically encrypted and so activities are not tracked and is a great tool for anyone wishing to access information that may not be approved by, for instance, local government. Also by using the Epic browser, those annoying adverts that are rife when searching online are blocked and this means that you are not forever trying to get them off your screen. One downside to searching using Epic is the speed, typically when searching for the pages you are looking for using Epic you may see a slightly slower result and the pages may take longer to load, a small price to pay for the added security. Considering this is a free download it is a great tool to add to your online security arsenal.

Epic has been having a massive battle with Google, who depend on their ability to sell ads for a large part of their revenue. Google has done its best to destroy Epic. Their behavior in this matter is very reminiscent of other IT giants when anything threatens their gold mine.

Given that Google has almost limitless resources, this is very much a David versus Goliath situation, so in addition to installing this browser, I do humbly suggest that you carry out all the other suggestions mentioned previously in order that you can be online anonymously.

In addition to its sterling work in preventing you from being tracked by Google, Epic has a built in a method of stopping canvas fingerprinting, a method of tracking discussed in the last chapter.

10. Use a VPN. This stands for Virtual Private Network. If you really want privacy, be prepared to pay from $5 to $10 a month for the use of a good VPN.

    A VPN is a private server that does the work on the Internet that you ask it to in such a way that your IP address is hidden. One of the most useful features of VPNs is that normally if you go to a web page using the HTTP:// protocol and you submit a password or carry out other secret processes, then the Internet traffic resulting from this is not encrypted. If you use a VPN, then all such activity that you may do on your browser is automatically encrypted. It is as though the protocol was https://

    VPNs are treated with the greatest suspicion by US authorities. If a VPN server is based in the USA, it is far more likely to be compromised than one based in other countries such as Sweden or Germany. Despite this, if your wish for anonymity is so that you can view child pornography or practice terrorism, then you will eventually get caught. The means by which online activity is tracked is forever becoming more sophisticated.

11. Mac Spoofer: MAC (Media access control) addresses are unique to each device and can easily be tracked. In order to mitigate against this, you can use a piece of software called a Mac Spoofer. There are a number of reasons to change or spoof your MAC address, the most obvious being to avoid network restrictions and giving you additional privacy.

    Another bonus with a spoofed MAC address is that it can present a viable solution to a broken router, by using a spoofed MAC you can still gain access to the internet. In order to change your MAC address, you should open your start menu, select your control panel, after launching your control panel then click on the network and internet option. Click on network and sharing center, usually the first option available and then click on it, this will lead you to your

communication/network setup and connections, select change adapter settings.

Select local area connections and click on properties and then on the Configure option, from the configure window look to the top right of the window where you will find the Advanced option, click on this, under the Advanced options you will see a smaller window headed Settings. Scroll down until you hit Locally Administered Address, click on it. Look to the text that will be in a yellow background and search for the text that will roughly match Change the MAC address used by the network adapter. Right next to the Settings window is a box marked Value. You will be typing a new combination of characters to spoof your MAC address.

It is worth saying that before you change the MAC address it would benefit you to check the combination of your original address. So now go back to the Start menu and click on it and there will be a search bar at the bottom below All Programs. In this search bar type cmd and then look to the top of the search results and you will spot something labeled cmd.exe, click on it. A new window with a black background will appear and will contain some text, there will also be a blank underscore that will be flashing on and off this is where you should type in getmac and hit enter. This will result in a list of Physical Addresses appearing, the first of which is your current MAC address. Now pull up the Advanced options window and in doing so you can change your MAC address to a new one and by following the format of your original address which will have 12 characters in total.

You can use letter combinations from A-F and any numbers, so under Value enter your new address but remember to maintain the format, for example, if the first 4 characters are A3-E2 then you can change them to E1-D2, by repeating this with all 12 characters you ensure you keep to the format required. Okay, the final step is to press OK on the bottom of the window, the Advanced option window will disappear from your screen and there will be movement in the Local Area Connection and for a short while a red cross will appear next to

Local Area Connections and will display the word Disabled, this merely means that the system is registering a change and after a few seconds this will disappear and your Local Area Connections will be Enabled. Congratulations, you have successfully spoofed your MAC address.

12. Get the TOR browser, you will not be disappointed. This is the main topic of this book, so I will not be saying too much about it now. The next chapter contains information about it, how to install it and use it. You will be grateful that you did, because then you will actually be able to browse the internet and be safe about it.

In addition, always make sure your antivirus and anti-Malware programs are strong and up to date. Below I will try to explain the difference between the two and what steps you should take when choosing the best product for you and your computer.

So, what is a virus and what is malware?? Well, malware covers a whole range of nasties that can affect your device. Spyware, that is software that is designed to gather information without your knowledge and also pass on this information to other parties. Adware is another form of malicious malware that is designed to generate ads in order to create revenue for its creator. The Trojan, as suggested by the name, is a harmful program that will access your software by misleading the user of its true intent and are generally spread by social interaction maybe an e-mail attachment that contains a routine form.

A virus, on the other hand, is a piece of code that can copy itself and cause harm to your device, so whilst all viruses are classed as malware, not all malware are viruses.

The main difference between antivirus software and anti-malware is that an anti-virus program is more likely to target the older more established threats like Trojans and viruses whilst the anti-malware software will be adapted to focus on newer up to date threats. Whilst your anti-virus software is working away to combat threats from malware you may contract from traditional sources such as email or a USB.

Which should you use?? The simple answer is to run the two programs side by side as when you try and combine the two elements you lose certain aspects, and since anti-malware is mostly lightweight and easy to run it is also designed to work alongside anti-virus programs to give you layered protection against both viruses and malware.

The best health care plan for your computer could include an anti-virus product such as Bitdefender, Norton by Symantec or Kaspersky Anti-virus which are the top three listed for 2017 by PCMag. For an effective anti-malware program try Hitman Pro, Malwarebytes, Zemena or Emsisoft. A final bit of advice when choosing your software, never trust unknown malware/adware or virus removal tools as they can also infect your computer and lead to the type of problems you are seeking to guard yourself against.

Chapter 4: The Tor Browser

TOR is the abbreviation for *The Onion Router*. At first, it was a global network of services developed by the US military so that Internet browsing and use could be performed anonymously. TOR sends Internet traffic as relays through a global network of thousands of servers to hide the location and activity of a client from surveillance and traffic analysis.

TOR servers, which provide the relays, are run by volunteers keen to protect online privacy and security. Rather than a direct connection with the source or destination of their communication, users have their network traffic pass through a large number of servers. The effect of this is to greatly confuse potential trackers.

Anyone who wishes to keep their Internet traffic out of the hands of advertisers, journalists and others, will benefit from the use of TOR. It is of great use for undercover cops working inside criminal organizations. It makes it to where the cops are completely undetectable as they continue their research.

TOR is a very useful tool for fighting censorship. It permits users to access destinations, which might otherwise be blocked. This is done while the privacy of the user is well preserved. Some foolishly regard the wish for online privacy as an indication of involvement in child pornography or terrorism.

Nothing could be further from the truth. A journalist living in a dictatorship would need online anonymity in order to protect his or her freedom and possibly life. They would need this anonymity to protect their sources.

TOR is of great use in the development of a new means of communication with inbuilt privacy. On the regular web, nothing is private. However, with TOR, you will be able to surf the web privately, not having to worry about anyone finding out what you are doing.

TOR has what are called *hidden* services. This allows users of the network to set up chat rooms. In these chat rooms, frank discussions can take place on matters such as rape, domestic abuse, all sorts of illnesses and

whistleblowing. Information, freely exchanged, which could be of great use to insurance companies, big business, and the media.

If someone is using TOR and someone tries to track them, then all that the tracker can see are random points on the TOR network. The user's computer cannot be identified. It will save you from getting hacked, which is a problem in today's society. You will be able to browse the web, without worrying about whether you will be attacked or not.

In order to use this network, it is necessary to download the TOR browser and to install it on your computer. Using the TOR system makes for slower browsing than normal due to a large number of relays that signals pass through.

These services are only available to TOR uses. Sadly, these services, although possibly created for the noblest of reasons, have been horribly abused. Various sites such as the Silk Road whose purpose was the selling of illicit drugs or the site which was busted by the FBI involving the largest child pornography ring that has been discovered set very bad examples. Despite these problems, TOR has been endorsed by such organizations as Indymedia for protecting their journalists and the Electronic Frontier Foundation for upholding online privacy.

Some large corporations use TOR commercially in order to analyze the behavior of competitors as well as to shield their own activity. TOR is better than most VPNs as it is impossible to determine the timing or quantity of a communication.

TOR is still used by the U.S. Navy and it is used by law-enforcement agencies during many operations where it is important not to leave a government IP address.

The more people who use TOR the better and the more secure it becomes. Any user's network traffic is hidden among the traffic of others using the network. A type of tracking tool, which TOR protects a user from, is called *Traffic Analysis*. This cunning method provides knowledge of the source, the destination, the time and the quantity of a communication and allows deductions to be made as to who is communicating with whom.

Traffic analysis works by focusing on the header of a *data packet*. Data packets have payloads, which could be an email, a video file or a PDF document. The payload is encrypted often but the header is not and therein lies a vulnerability. Clever analysis of headers can reveal a wealth of information such as the source, destination, time and size of the payload.

A problem for those who wish for privacy is that it is essential for the computer of those who receive your communication to get the information contained in the header. This information can be obtained by others using sophisticated software. These others include ISPs, law-enforcement agencies if they are tracking you, and other trackers.

TOR reduces the risk of detection by all types of traffic analysis through its distribution of communication through multiple servers, the idea being to deliberately prevent trackers from knowing where the communication has come from or where it is going.

The means by which this path of nodes or servers is constructed is very clever. It is done server by server with encryption as it goes along. No server or relay knows the complete path.

Completion of a circuit allows all sorts of applications to be used on the TOR network. TOR only works on TCP communication, which has *SOCKS* support. Socks is an Internet protocol which exchanges data between a client and server through a proxy server. This is a server that is a link between networks.

TOR is brilliant but it is foolish to think that if you use it you are completely anonymous. If you, for any reason, come to the attention of the law, then they will eventually get you. All TOR can do is slow down this process.

One of the ways in which organizations like the FBI use the TOR network to catch the bad guys is to join TOR. The services of FBI servers are used as part of the TOR network unbeknownst to TOR.

Despite this, the big arrests of the child pornographers, which was mentioned before, was not done via this route but by the injection of malware into the browser of some abuser who had let his guard down. The

browser is the weak point as regards law enforcement and other tracking. Attacks on the browser are called "*Man in The Middle"* attacks.

Law-enforcement agencies have to be very careful how they operate because the users of TOR are among the most computer savvy people in the world and if it became obvious that law-enforcement was targeting too many of them then they would take countermeasures which would make TOR users much safer and consequently the targets of the law-enforcement more difficult to catch. Law-enforcement is consequently very careful to cover its tracks and only go after the real criminals.

Next, we discuss how to install the TOR browser.

The TOR browser is a version of the open-source Firefox browser. The installation of this browser is quite easy. Google, 'download TOR browser.' You will come to the download TOR website. Click on that and follow instructions. You will receive a menu of TOR downloads for the various operating systems that are, of course, Windows, Apple, Linux, smartphones and one labeled source code.

Pick the one you want. Assuming you picked Windows, you can select the folder that you want to place the browser in. Once you have done that, press install and the process of installation is automatic.

There is one final window you have to work on. Press the upper button unless your Internet connection is censored, filtered or proxied. Most of us just press the upper button which says *connect*. The bottom button says *configure*. Be sure and read the warnings on the TOR window.

If you press to connect, the connection is not instantaneous but when it is complete, you should have a green window with some safety warnings and information about the TOR project. To ensure that you are connected to the Tor network, put www.whatismyip.com in your address bar and press enter.

You will notice the slowness of the browser in comparison to the usual speed of Firefox or Chrome. Pay particular heed to the warnings that TOR urges you to follow. One of them is that you should not *Torrent* when you download files. If you do that when downloading a file, it will give a virus, or a hacker, easier access to your computer. The next chapter will deal with the *Deep Web* which the TOR browser is specifically designed for.

Chapter 5: Secrets of the Dark Web

Dark web: Many people confuse the *Dark Web* with the *Deep Web*. The dark web, refers to the encrypted network between the servers of TOR and those using them, the clients.

On the other hand, the Deep Web is composed of all the files on the Internet, which cannot be indexed by normal search engines such as Google and Bing. The Deep Web has been estimated to comprise 99% of all Internet content. There are estimates that it comprises 7500 Terabyte of data.

Most material on the Deep Web is not very interesting. For example, newspapers maintain Deep Web databases of stories that are not published. Much other equally boring data exists. For instance, the sales records of the billions of transactions carried out by businesses would be on Deep Web sites. The Deep Web is mainly benign and boring.

The Dark Web is far more interesting. Just about anything you could want is available on the Dark Web. Among the things that you can get:

1. **Banned books.**

Whilst most people believe the Dark Web is filled with pornography, drugs and all things criminal it is a lesser known fact that there are an awful lot of bibliophiles on the Dark Web. In 2011 The Dread Pirate Roberts who founded the original Silk Road began his drug bazaar book club and is quoted as saying, “Knowledge is power, and reading is one of the best ways to expand your knowledge. Each week we will select a reading designed to expand our understandings of the issues that face the Silk Road community and have a group discussion of this material. My hope is that a high level of discourse will be fostered, and as a community, we can become strong in our beliefs, with a coherent message and voice as the world begins to take notice.”

And of course, the world did take notice and Roberts was arrested, not for his book club, but for drug trafficking and money laundering charges. Silk Road was closed and its book club was no more. But they were not to be silenced, only a month later and Silk Road was up and running again, as

was the book club being moderated by a Silk Road senior moderator by the name of Inigo, until Inigo himself was arrested and the book club decided to cut its ties with Silk Road and continue in a private chat room whilst still upholding the legacy of Inigo, after all. Knowledge is power!!

2. Copied credit cards.

The Dark Web is like a shopping mall for cybercrime. Not only credit cards but spammer lists, phishing kits and all the tools needed to carry out all manner of cybercrime are available. Large batches of credit cards from US retailers appear on what is known as a carder forum, it is like Craig's List for hackers where cards backed up with customers details are being traded for as little as a dollar a card.

3. Fake passports.

There are many opportunities for obtaining fake passports on the Dark Web, the quality, however, is varied. Many people claim to have purchased and used these copies on many occasions, seemingly enabled by the sellers claim that they have insiders in various departments that enable them to enter the false details into legitimate channels. Most of the time, these people are here illegally and need a respectable way to travel, thus resulting in them finding these people that sell the illegal substances.

4. Illicit drugs.

Though only a small percentage of illegal drug purchases are made online the figure is growing, and growing fast, thus changing the whole process of drug dealing in the process. Sellers are now more focused on selling a better quality of product at a more competitive price and thus creating a reputable brand name. Estimated turnover in 2012 was $15m - $17m yet by 2015 this had risen to $150m - $180m.

5. **Hackers**

Want to check out what your ex is up to?? Or maybe bring down a major company and bring them to a halt, there are a whole bunch of sites on the Dark Web where you can find people who will do whatever you want them to do.

6. Burglars

Not quite so prevalent, but there are reports of sites on the Dark Web where you can employ someone to steal an order. You place your request with as much detail as you can and he will then steal said item and send you a picture to prove it. Apparently, he also has a list of items for sale that originated when people ordered the thefts and then never followed through with payment.

7. Illegal betting and match fixing

In these days of highly regulated betting practices, especially since the birth of online betting that has grown since its conception in the late 1990s and according to Statista accounted for a volume of $46 billion in 2016 and is predicted to grow to $56 billion by 2018, it is getting more difficult to place illegal bets. On the Dark Web however you can place all manner of illegal bets and match fixing is rife. With the click of a mouse, you can basically do as you please.

8. Hitmen

Now, this is dark. The availability to hire a trained gun is widespread, and whilst not cheap, it is not too highly priced to deter a serious buyer. One site is purporting to advertise an assassination in the US or Canada for $10,000 and $12,000 in Europe, according to the Mail Online. Some of the slogans and marketing techniques are truly chilling. One self-styled assassin claims, “I do not know anything about you, you do not know anything about me. The desired victim will pass away. No one will ever know why or who did this. On top of that, I always give my best to make it look like an accident or suicide” It is completely terrifying to know that there are people out there that support something like this. However, you will be surprised to find that a person that is close to you can even be in on this type of activity.

Almost all sales are via “crypto markets” the Black Webs equivalent to Amazon and E-bay, employing a similar feedback method and allowing customers to rate sellers, products and allow other buyers to base their purchase choices on informed information. Administrators take a cut from each sale and pay moderators (in bitcoin of course) to handle forums and complaints.

9. **Weapons**.

It is rumored that The Armory is the biggest and most known online marketplace for weapons, requiring a minimum order of $1050 it purports to stock around 400 items for sale, specializing in firearms that are untraceable or have a fake serial number. Also boasting a military section they appear to be one of the biggest weapons traders online and have an active community following.

These must be paid for with *Bitcoin*, which is the online currency. Bitcoin is a peer to peer system created in 2008 and is used to pay online transactions without the use of a central trusted authority. Since its creation, it has evolved into something far beyond a simple currency. It has its own community of users and it is also an investment vehicle. What makes bitcoin work is the massive peer to peer network and the consensus involved that enables a payment system where payments cannot be reversed, accounts cannot be frozen and this leads to much lower transaction fees.

Bitcoin, as with the Internet itself has no central owner or authority and is primarily governed by the developers who put their time in to ensure that Bitcoin works as it is only in their interest to ensure that the right decisions are taken. The amount of influence their input carries is based on the amount of computing work they donate to the network.

Similarly, some users put in work to aid the smooth running of the peer to peer network and are rewarded with Bitcoins that can be spent online. This is a simple form of mining, the term used to describe obtaining bitcoins. The best way to understand bitcoin is to get some and experiment, there are various ways to do so and the information is out there to help you.

Some idiotic people put sensitive information, such as nude photographs, in the Deep Web. They think it is secure. It is not!

A classic example is the Ashley Madison site, which was created for bored spouses who wanted extramarital affairs. A hacker broke into that site and 10 GB of data from the site was placed on the Dark Web and thus became available to users of TOR. The hack was discovered by a journalist called

Brian Krebs who had written for years about internet security and the theft of data from major companies in the form of a popular blog. He had investigated various firms like Dominos Pizza, Tesco, and Adobe and he received an anonymous link to caches of data stolen from a Canadian firm called Avid Life Media (ALM) of which he was vaguely aware. Since 2008 they had run a well-publicized dating site for married people.

Promising 100% discretion at the time of the tip-off they were currently claiming to have a membership of 37.6 million members worldwide. However, simply by following the links, he had been sent Krebs found himself looking at actual credit card details for real members of the website that would previously have promised total discretion. Among documents, he found not only a list of senior executives but the personal phone number of the CEO. As a consequence, some users of the Ashley Madison site have been subject to ransom demands, and even a small number of suicides have been reported. This was possibly the largest most destructive example of how, no matter how careful you are with your internet traffic, your online presence is something you should always mindful of and be aware that outside influences can come into play and expose personal details.

If you wish to see some of the material on the Dark Web then log onto TOR and put *thehiddenwiki.org* into the address bar and press enter. A long list of sites you can visit is displayed. I won't ruin your experience by telling you what is there but do advise you to take extreme caution and have very good malware protection.

Depending on what you intend to do and your state when you visit any of these sites, it has been recommended that you put masking tape over the webcam on your computer. If you don't do this, prying eyes may witness you and your home. This is definitely not in your best interests!

Chapter 6: How to Surf the Web Like a Hacker

First, let me explain the various forms that hacking can take.

Hacking can be a serious crime, and it can affect people who are not necessarily the intended victim of the crime. The effects can manifest in a number of ways and be disastrous.

The first way a hacker can harm you is by identity theft. Identity theft can be devastating for its victims, hackers can steal both identifying and financial information and wreak havoc on their victim's lives. More often than not, the hacker is doing this for a reason. They could simple enjoy the thrill of it by using the details they have garnered so they can make unauthorized purchases. They can complete wreck your credit as they charge items on an existing credit card, even ordering new credit cards and subsequently new accounts and sometimes severely damaging their victim’s financial status. In the best-case scenario, when the crime is discovered early, it can still lead to months, or even longer, of worry and work to recover the situation. Sometimes, multiple false IDs will have been generated using the victim's data and all activity involving these IDs will need to be followed and investigated.

Hacking of Government and corporate websites can be devastating and at times lead to a total shutdown of a site until any security breaches and damage to the site has been assessed and corrected. The damage that can be caused by these shutdowns can be long-lasting and lead to huge losses financially. The shutdowns can also occur if the website has been targeted by a “denial of service” attack, put in layman’s term the website is targeted and bombarded with false traffic that leads to it being unable to handle requests from genuine traffic.

Hackers may also resort to placing malware and viruses on computers. Often these programs are masked by a useful program and this leads to installation of the harmful portion simultaneously. Some software will then go on and create the illusion of a computer virus in order to convince the user to purchase fake antivirus protection or, alternatively the malware will be programmed to record keystrokes in order to steal passwords and other

financial information. These harmful programs can even allow a hacker to take remote control of a computer and then perform nefarious activities such as a denial of service attack and make it appear to have been performed by the infected computer.

A little-known fact about hackers is that not all hackers are malicious. Sometimes known as 'Ethical hackers" or "white hat hackers" often assist government and other possible targets to improve their security and take all possible measures available to them to prevent major security holes from being exploited. These "good" hackers are a major tool in the overall fight against all matters of identity theft and are striving to reduce the number of instances.

If you Google,' *Surf the web like a hacker,'* you will get all sorts of information. Some articles will give you tips about speeding up your surfing while others will tell you how to defend yourself against hackers.

A hacker is usually a very clever person who tries to get into the computers and computer networks. There are many people who do not want the hacker to do this, but in situations you cannot ward against them unless you have a very good blocker on your computer. Hackers crave anonymity. They crave the attention they gather when they do a job successfully. Their activity is usually illegal, and if they are found out, it will cause them to result in paying a hefty fine and prison sentence. However, there are some hackers out there that do not get caught—ever. They know the internet like the back of their hand, and they can successfully filter through the pages without being detected.

Many hackers do what they do as a challenge. It is the same way that some people enjoy doing crosswords or Sudokus. Like fans of these more familiar activities, more and more challenging hacks are required by hackers doing that activity for pleasure. They enjoy the thrill of being able to get into places normal people cannot.

Unfortunately, some hackers have criminal motives and you need to protect yourself against them by installing malware and other virus protection onto your computer. Irrespective of their motive, whether it be for the intellectual challenge or for more sinister reasons, once a hacker has access to the device or network, they can do enormous damage.

They may plant programs called Trojans or backdoors into the computers of its victims. When they accomplish this, it will relay information back to the hacker. They will be able to get any type of information from your device with as little effort as clicking a button. Hackers sometimes work alone. They feel the need to work alone, as they will only have to rely on themselves. Occasionally, they will belong to collectives, but you will not find this often.

One of the best-known hacker collectives is the one called *Anonymous*. Wikipedia has a very interesting article about Anonymous and I suggest that you read it. The Scientology organization suffered greatly at the hands of Anonymous, as have other organizations which have annoyed Anonymous. In the wake of the Charlie Hebdo shootings in January 2015, Anonymous released a statement on Twitter condemning the attack and declaring a war on the terrorists responsible. He vowed to shut down any associated social media accounts. It is reported that on the 15th of January they did indeed manage to close down a website belonging to one of the groups believed responsible for the attack, but critics have pointed out that by closing down extremist's websites you then make it harder to track their activities.

Earlier in this chapter, the desire of hackers for their activity to be anonymous was mentioned. By use of the TOR browser, anyone can achieve the anonymity that hackers crave.

Conclusion

So, now you are armed with the knowledge you need to enter the world of the Dark Web. I've give you the steps to do this as safely as possible and to conduct yourself in a way that will not put you or your device in peril. Also, here are a few more key tips to remember, which are listed below.

1. Providing you are using the Tor browser, you could actually be safer on the Dark Web than your normal internet activity. It comes preconfigured to provide protection against privacy threats that are not addressed by normal browsers.
2. If you do register on a site don't use your real e-mail address, your real name or username. Create a throwaway identity, and whatever you do refrain from using a credit card, you have absolutely no recourse and you may have some awkward explaining to do when your charges appear.
3. If you are concerned that your activity online may alert a higher authority then relax, there is so much activity on the Dark Web that, unless you live in a particularly authoritarian country, you are highly unlikely to raise a flag and attract unwanted attention. If this is a concern you can always connect to a VPN before connecting to Tor.
4. If you really must download something, and please don't unless you really must, then protect yourself with a really good anti-virus such as VirusTotal. Anything that you download can effectively hurt your device. You must be totally sure that you are going to be safe from virus.' If you get a warning sign, turn back. Do not go forward with the download.
5. And finally, exercise common sense in everything that you do. As in any other activity you undertake, remember, if it seems too good to be true, it probably is. You do not want to risk yourself, or your system. If there is some random stranger being overly friendly, is he now your next best friend? Probably not, remember your own common sense and natural instinct. It will serve you well if used correctly and can provide a greater protection much more than any

anti-virus or defensive software (but obviously you still need these protective tools).

Just remember that once you are using Tor and its hidden services, you are equipped to navigate the web on a day to day basis, so build your skills and use them well.

The ability to surf the Internet anonymously is of ever increasing importance. It gives you the ability to do the things you would not normally accomplish, giving you the confidence boost you did not know you needed in your researching skills.

Why this so important and how to do it is the essence of this book.

This book has thoroughly covered the means by which this can be done, and be accomplished successfully.

It has demonstrated how to stay anonymous as you use this technology, which plays such a dominant part in our lives. It is hard to stay anonymous in this day and age, and TorBrowser helps with that.

It has repeated warnings about steps you need to take before you venture into the Dark Web. The Dark Web is a dangerous place, and if you do not know how to venture into it carefully, you can find yourself in peril. Now that you know about the dangers you can face, you can plan against them.

Happy Surfing!