THE DEEP AND DARK WEB GUIDE

SAFELY EXPLORE THE HIDDEN INTERNET

BY GAVIN PHILLIPS

The Deep and Dark Web Guide

Safely Explore The Hidden Internet

Written by Gavin Phillips

Table of Contents

Lesson 1 - Introduction to the Deep and the Dark Web

In this free MakeUseOf guide, you will learn everything you need to know about the deep and the dark web, including how to access them, the differences between the deep and the dark web, and why you might want to use the dark web instead of the regular internet.

Disclaimer: *If you follow the instructions in this guide, you should be safe while using the dark web. That said, MakeUseOf and I are not responsible for any websites, content, or otherwise you encounter while using the dark web.*

Introducing the Deep and Dark Web Guide

Let's break the guide down:

Lesson 1: What is the deep web, and is it any different from the dark web?

Lesson 2: Why would you access the dark web and is it illegal to do so?

Lesson 3: How to access the dark web securely, including how to install a VPN.

Lesson 4: Your hands-on guide to accessing the dark web using Tor and a look at the alternatives.

Lesson 5: Navigating the dark web, using dark web search engines, and services and sites you should check out.

Lesson 6: Your Deep and Dark Web guide roundup.

Within each lesson, we'll provide a couple of small tasks for you to complete for the following lesson, plus a few handy links for you to expand your reading—but only if you want to!

What Is the Deep Web?

The deep web comprises all of the "hidden" internet that's inaccessible using a regular search engine, in a regular browser, to "regular" internet users.

The inaccessible internet isn't as exciting as it sounds. It includes banking portals and login pages, academic journals and studies, government gateways, tax forms, long-forgotten secure databases, and so on. Anything that Google and other search engines do not index. (Check out these **search engines that let you explore the deep web**!)

But the deep web is important. It forms a vital part of the internet as we know it, keeping certain forms of data secure from prying eyes. More than that, it is enormous.

According to Dutch researcher Maurice de Kunder, the visible web contains around 5.24 billion web pages, but no one knows the true size of the deep web. Estimates range from around 10 to 500 times bigger than the regular internet. Even at a conservative estimate, it is a staggering volume of data.

The rule of thumb: if you have to log into an account to access a page, the information you are accessing is on the deep web.

What Is the Dark Web?

The dark web is an "overlay network" that you can only access using specialized software, such as the Tor Browser. (More about using the Tor Browser to access the dark web in Lesson 3!) An overlay network works on top of the regular internet, but requires special software to access.

Websites on the dark web require your browser to use specific security and privacy configurations that allow it to communicate with the network of anonymous websites on their anonymous servers.

While the deep web is huge, the dark web is tiny. It is difficult to gauge the size of the dark web because most dark sites are extremely well-hidden (you cannot find them unless you are told where to look), but estimates put the number of dark sites at between 200,000 to 400,000.

Of those, a huge amount are hidden services that you will not find, and the remainder mainly consist of ransomware ransom notes demanding payment to unlock infected machines.

Still, there is plenty of interesting stuff on the dark web to browse.

Are the Deep Web and the Dark Web the Same?

No.

The deep web refers to other websites whose contents are not indexed by search engines. The dark web is a network of anonymous websites.

When people talk about underground forums, hackers, assassins, purchasing stolen credentials, and credit card trading, they're talking about sites and services hosted on the dark

web. For instance, security researchers found **35 million US voter records for sale** on a dark web forum.

How Does the Dark Web Work?

The majority of people access the dark web using the Tor network. Tor is an acronym for "The Onion Router." Just as an onion has many layers, so does the Tor network. Sites hosted on the Tor network use the ".onion" domain. However, onion sites don't use the same DNS (Domain Name System) that the clearnet (i.e. the "regular" internet) uses.

Normally, when you type a URL into your address bar and hit Enter, your browser uses the DNS to look up the IP address of the URL and take you there. If you try that with an onion domain in a regular browser, you'll see nothing but an error.

How Tor Works: 2

Tor node
unencrypted link
encrypted link

Alice

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Jane

Dave

Bob
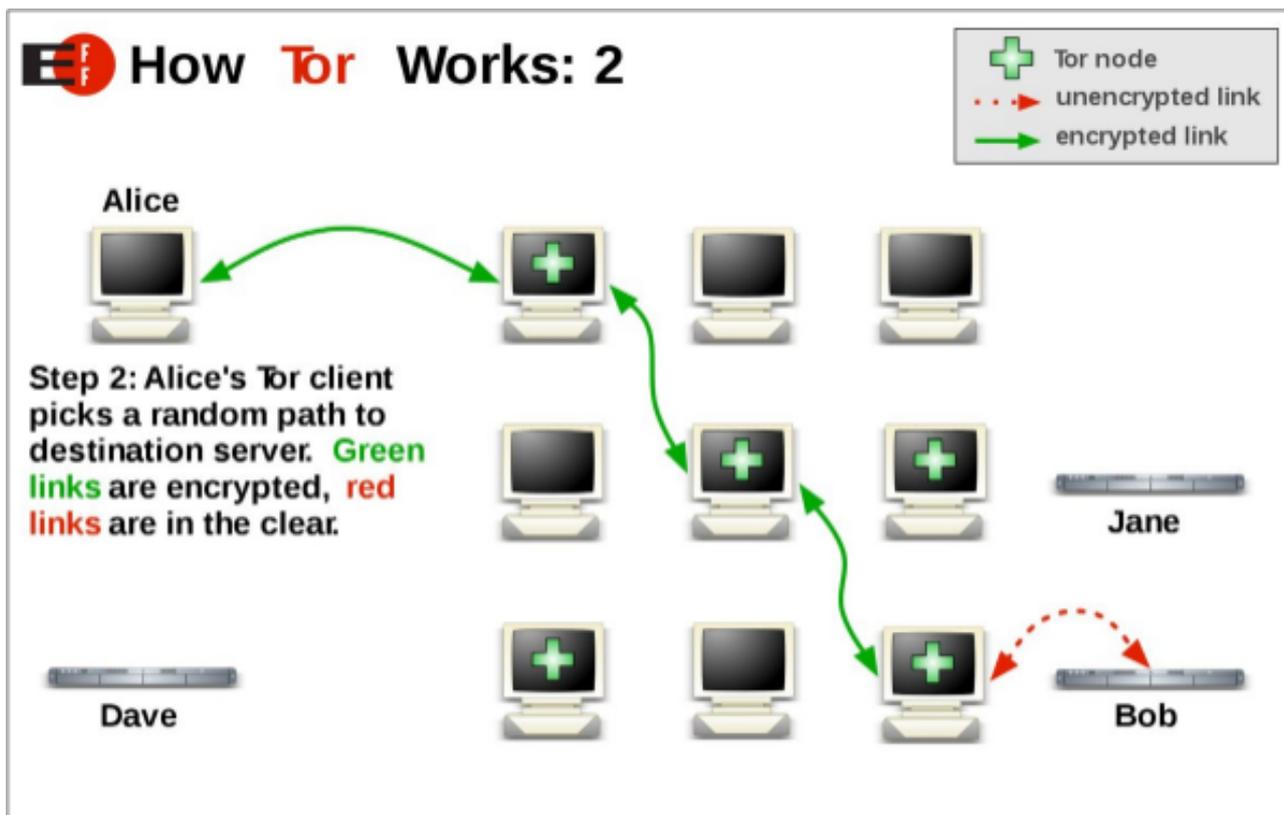
The structure of the dark web is meant to keep its sites, services, and users anonymous. For instance, when you use the Tor Browser to access the dark web, your internet traffic moves through several anonymous nodes between your computer and the onion site you want to visit.

How Tor Works: 3

Legend:
- Tor node
- unencrypted link
- encrypted link

Alice

Step 3: If at a later time, the user visits another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.

Dave

Jane

Bob
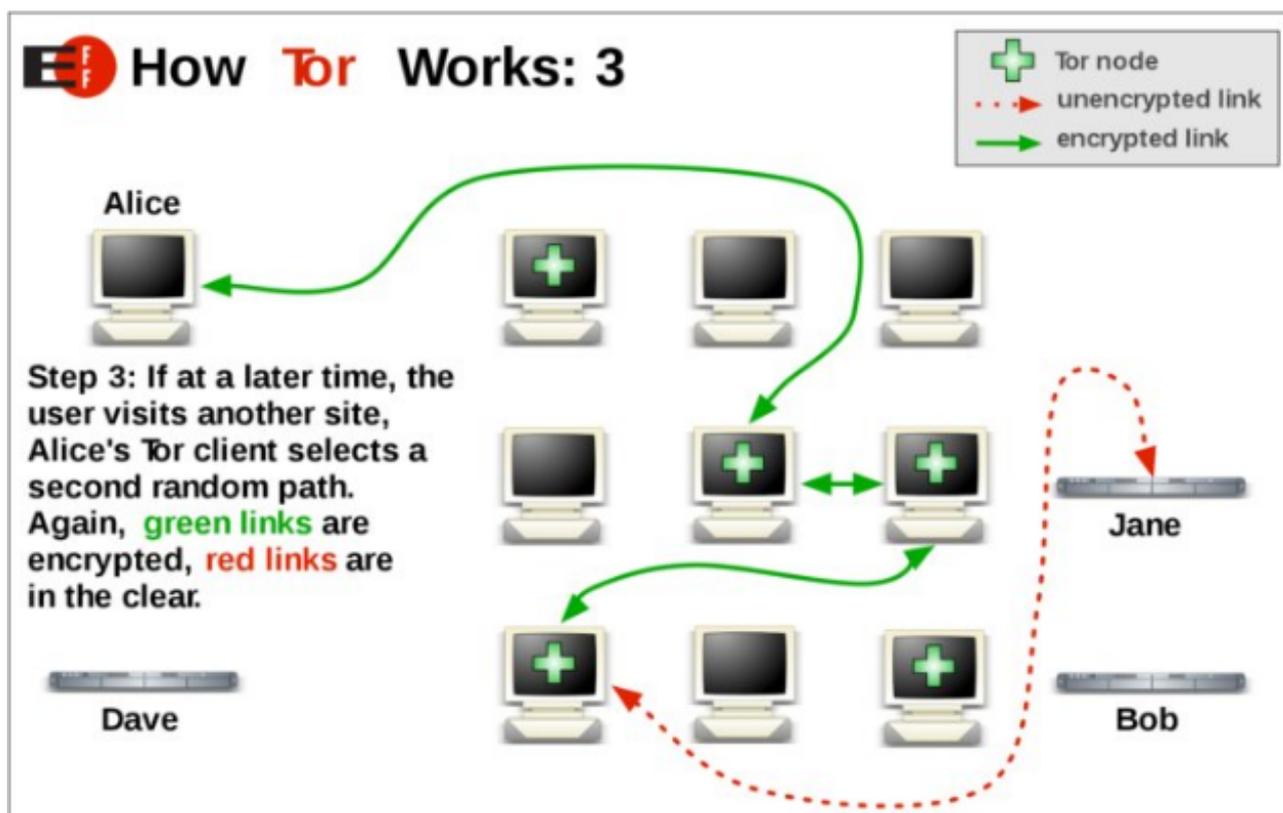
We'll explain Tor, onion routing, and the dark web in greater detail in Lesson 3. For your own privacy and security, we advise waiting until then before trying to access the dark web.

The Deep Web Is *Deep*

When people talk about the deep web, they usually mean the dark web. The rest of this guide will be about the dark web, so from here on out, unless the deep web is specifically mentioned, the following lessons will all focus on the dark web.

Before the next lesson, please:

‣ Look through the guide itinerary and figure out what interests you most!

In the next lesson: Learn why you might want to use the dark web, whether the dark web is safe and legal, and what you can do on the dark web.

Lesson 2 - Why Would You Access the Dark Web?

What is actually on the dark web that makes it so interesting? One common misconception is that everything on the dark web is illegal, or that even accessing the dark web itself will land you in trouble.

In this lesson, we'll explore why you might legitimately want to access the dark web, whether the dark web is safe, and most importantly, if accessing the dark web is legal.

Why Would You Access the Dark Web?

The primary reason for anyone accessing or using sites and services on the dark web is anonymity. A modern computer connected to the internet gives away information. Information about where you are, who you are, the things you enjoy, your dislikes, your family, and much more. The internet hoovers up information and keeps hold of it. And once it has the information, it is extremely difficult to remove it.

Privacy and anonymity don't mix well with the internet. At least, with the current structure of the internet. At some point, we all decided that we like our internet services free at the point of delivery. **The consequence is tracking, profiling, and targeting**. The dark web doesn't have advertising tracking. It doesn't profile your browser fingerprint to match your internet activity across different sites.

The dark web, then, allows you to use the internet as a truly anonymous individual. Within the sphere of privacy and anonymity, the dark web creates opportunities that would otherwise fail on the clearnet. Obviously, that means some illegal activity can flourish (more on this in a moment), but there are numerous legitimate reasons to access the dark web. For instance:

‣ For security research on underground forums

‣ For undercover law enforcement

‣ To make an anonymous tip (several major publications operate anonymous dark web tip boxes to protect the privacy of the tipster or whistle-blower)

‣ To access censored information; **numerous governments heavily restrict internet access and content**

‣ Hide all of your internet activity from your regular ISP (within the Tor Browser)

More reasons exist. But I'm sure you note the core tenet of the dark web running through these reasons. That's right: the dark web is a tool for privacy and anonymity for millions of global users.

Are the Deep Web and the Dark Web Safe?

The **deep web** is safe enough. You cannot access much of it, and what you can access is largely secure. For instance, you would hope your banking portal isn't going to expose you to malware, or that an Internet Archive cached page isn't hosting something nefarious.

I will counter that with the caveat that you should always browse the internet with an up-to-date antivirus suite. **A Malwarebytes Premium subscription is a wise investment**, too.

The **dark web** is a different kettle of fish. Privacy and anonymity are vital to the dark web. Security, however, is multifaceted. You should approach content on the dark web with caution. There are a few security issues to consider before you start clicking on links and finding onion sites:

‣ **Suspicious links:** The first thing to consider is links. If you start clicking on links, you may encounter illegal content, content you might not want to view.

‣ **Hackers:** They are real and can cause substantial damage.

‣ **Law enforcement:** I previously mentioned undercover law enforcement; the dark web is privacy and anonymity focused, but it isn't impenetrable. Some of the biggest busts on the dark web came from the dedication of undercover law enforcement officers infiltrating popular forums and marketplaces full of illegal activity.

‣ **Criminal activity:** Following on, criminals do use the dark web to buy, sell, and test their malicious activities. A site that appears perfectly normal may have a dangerous underside. You might be exploited, lose money, private data, control of your computer, and so on.

The dark web doesn't have to be unsafe. But you should approach it with caution. Check Lesson 3 and Lesson 4 for vital information about staying safe on the dark web!

Is the Dark Web Illegal?

No, the dark web itself is not illegal.

However, you can find illegal content and engage in illegal activities on the dark web. If the activity is illegal in the jurisdiction from which you access the dark web, it remains illegal online, too.

However, one caveat: Most people use the Tor Browser to access the dark web, and the Tor network uses strong encryption to protect users and their data. Therefore, if strong encryption is illegal in your jurisdiction (e.g. China), then accessing the Tor network is also illegal by extension.

Unsure about the status of encryption law in the country you are visiting? Check out the **Crypto Law Survey** for the encryption import status. The **GP-Digital World Map of Encryption Laws and Policies** is handy, too, as is the **BestVPN Are VPNs Legal In Your Country** list (featuring 196 countries).

What Can You Do on the Dark Web?

The dark web is host to many "regular" and non-criminal sites. Here are a few examples:

‣ **Sci-Hub** is a scientific paper platform with a mission to liberate scientific knowledge from across the globe. Sci-Hub hosts more than 50 million academic papers on a vast number of subjects, and you can access it all for free (it goes without saying that we do not condone copyright infringement).

‣ The Pulitzer Prize-winning **ProPublica** hosts a dark web version of its main site, complete with a secure and confidential drop box.

- **Facebook** hosts an onion site, allowing access for users in countries with censorship.

- Various VPN and email providers host active dark web sites, including the extremely secure **ProtonMail**. (Learn how to install a secure VPN in Lesson 3!)

What Are You Looking for on the Dark Web?

Before the next lesson, please:

- Consider what it is you expect to find or hope to use the dark web for.

- Update your antivirus. I'd also urge you to grab a Malwarebytes Premium subscription, or at least start the free trial.

- Check the legality of using the Tor Browser in your jurisdiction.

In the next lesson: Learn how to choose and set up a VPN to increase your security and privacy while browsing the dark web, how to avoid the really bad stuff, and how cryptocurrency figures in all of this.

Lesson 3 - Using the Dark Web Securely

Security is of the utmost importance while browsing the internet, especially on the dark web.

In this lesson, we'll explain how a VPN drastically increases your security on the dark web, how to steer clear of illegal sites on the dark web, and whether you should ever purchase something on the dark web using cryptocurrencies like Bitcoin.

Using the Dark Web Securely With a VPN

A Virtual Private Network (VPN) is a secure tunnel between your computer and the internet. No one can look into the tunnel, making your data secure. You can install a VPN on your desktop, smartphone, and even a router.

Once you install a VPN, your dark web traffic has an additional layer of security from prying eyes. The VPN software encrypts your data as it leaves your device. The data then travels to your ISP server, and then to the VPN server. The VPN server decrypts the data and releases it to the wider internet as usual. To outsiders, your activity looks like it belongs to the VPN server rather than your home computer.

You should always use a paid VPN rather than a free VPN. Most free VPNs log your data, defeating the purpose of using one if privacy is a concern. Should the government request it, a free VPN could give up those logs and lead them to you. Paid VPNs don't need to log your data for advertising or resale purposes, thus are safer.

Two of our favorite VPN providers are ExpressVPN and CyberGhost. Both have a long, respected history of keeping your data private when it matters.

Use **this link** to get three FREE months of ExpressVPN when you subscribe for a year, or **this link** to get two FREE months on top of an annual CyberGhost subscription.

VPNs are not just for when you want to access the dark web. They are an extremely useful privacy and security tool that anyone can use. Want to know more? Here are several **reasons why you should use a VPN at all times**.

How Do You Install a VPN?

We've written step-by-step guides for installing VPNs on various devices:

- **How to Set Up a VPN in Windows 10**

- **How to Set Up a VPN on Your Mac**

- **Everything Linux Users Need to Know About Installing a VPN**

- **How to Set Up a VPN on Android**

- **How to Set Up a VPN on Your iPhone or iPad**

- **How to Set Up a VPN on Your Router**

- **How to Turn a Raspberry Pi Into a VPN-Secured Travel Router**

Once installed, sign in using your credentials and always make sure the VPN is on before accessing the dark web.

Avoiding the Bad and Illegal Side of the Dark Web

It is no secret that you can buy all manner of things on the dark web. These illicit marketplaces are known as "darknet markets." Fortunately, visiting a darknet market isn't illegal, and you usually have to create an account to even begin looking at vendor listings.

In fact, most of the disturbing and illegal content is hidden away. You won't find a link to such a site unless you are actively searching for it and know where to look.

The most important thing is to move slowly. If you are unsure about where a dark web link might take you, don't click it. Some links may even lead to malware, but you can mitigate those risks with a good, up-to-date antivirus solution.

Dark web directories can be useful for checking where a link leads. For instance, Tor Browser users can use Daniel's Onion Link List Raspberry Pi Directory. Copy the link you want to check out into the "Onion-Address" box and see what it returns. **Daniel's Onion Link List** gives a brief site description, if available, plus a last seen and last tested date.

Should You Buy Anything on the Dark Web?

Well, it depends on what you want to buy. If you're buying a VPN or email service subscription, go ahead. However, do not use your regular banking details. If you purchase anything—and I mean, anything—you should use a cryptocurrency to do so.

Cryptocurrencies, like Bitcoin, are almost completely anonymous. Because there are significantly fewer protections in place on the dark web, entering your banking credentials is a massive no-no.

Purchasing Bitcoin and other cryptocurrencies is incredibly easy. Our sister site, **Blocks Decoded**, makes understanding and using cryptocurrency easy. Check out:

▸ **How to Buy Your First Cryptocurrency on Coinbase**

It is better to lose some cryptocurrency than it is to lose your banking details. However, be careful. There are no chargebacks, refunds, recourse, or customer service with cryptocurrencies.

Proceed With Caution on the Dark Web

If you take the proper steps, the dark web is a relatively safe place to explore. Those steps include:

▸ Updating your antivirus (and considering installing **Malwarebytes Premium**)

▸ Installing an ExpressVPN or CyberGhost VPN client

▸ Checking links before you click them

▸ Using cryptocurrency in place of regular money to make purchases

Before proceeding to the next lesson, please:

▸ Consider signing up for and installing a VPN.

In the next lesson: Learn how to install Tor Browser and how to access the dark web.

Lesson 4 - Accessing the Dark Web

Welcome to Lesson 4 of your free introduction to the deep and the dark web. In this lesson, you'll learn how to access the dark web using the Tor Browser.

How Do You Access the Dark Web?

Accessing the dark web is surprisingly easy. The majority of users access the dark web using the Tor Browser. Some alternatives include I2P, Freenet, GNUnet, and ZeroNet.

Pros and Cons of Tor

Tor has a lot going for it in terms of network reach. Compared to alternatives, Tor has a large user base which helps your traffic blend in. Furthermore, Tor allows you to access regular sites on the clearnet while staying protected by Tor Browser's integrated privacy settings.

The Tor network and Tor Browser are under constant development by a dedicated team, which is another positive.

However, **there are potentially insecure exit nodes that could intercept your data**. The Tor network and the hidden services hosted on it are heavily scrutinized by law enforcement. Also, tiny changes can make you more vulnerable to identification. For instance, running your Tor Browser window at a custom size increases your chance of "standing out in the crowd" versus running it at the default size.

Accessing the Dark Web Using Tor

Tor software directs web traffic through a worldwide system of interconnected relay nodes. This is known as "onion routing" because your data passes through many layers. Tor encrypts all network traffic, including the next node IP address, and encrypted data passes through multiple randomly selected relays.

The final relay node decrypts the entire package, sending the data to its final destination without revealing—at any point—a source IP address.

## Installing Tor Browser and Accessing the Dark Web

Here's how you do it.

1. Start and login into your VPN.

2. Head to the **Tor Project**.

3. **Download the Tor Browser** for your operating system. (The browser is available for Windows, macOS, and Linux.)

4. Double-click the Tor Browser file to begin the installation process. Follow the on-screen directions. The folder location of the Tor Browser is not important.

5. Once the installation process completes, head to the Tor Browser folder. (The one just created during installation.) For instance, I head to C:/Tor Browser.

6. Select **Start Tor Browser**. Choose **Connect**.

7. If there is a Tor Browser update available, install it before progressing. **This is very important**. A poorly configured browser could leak your data.

That's it! You're about to start browsing the dark web. You should not mess around with the Tor Browser settings; they work out of the box, and if you mess with them, you could inadvertently expose yourself.

Want to check if it is working? Here is an onion link for The Hidden Wiki: **http://zqktlwi4i34kbat3.onion/wiki/index.php/Main_Page**. Incidentally, The Hidden Wiki is a handy place for first-time dark web users, full of interesting and helpful links (and some fairly dodgy links further down the page, so don't use those!).
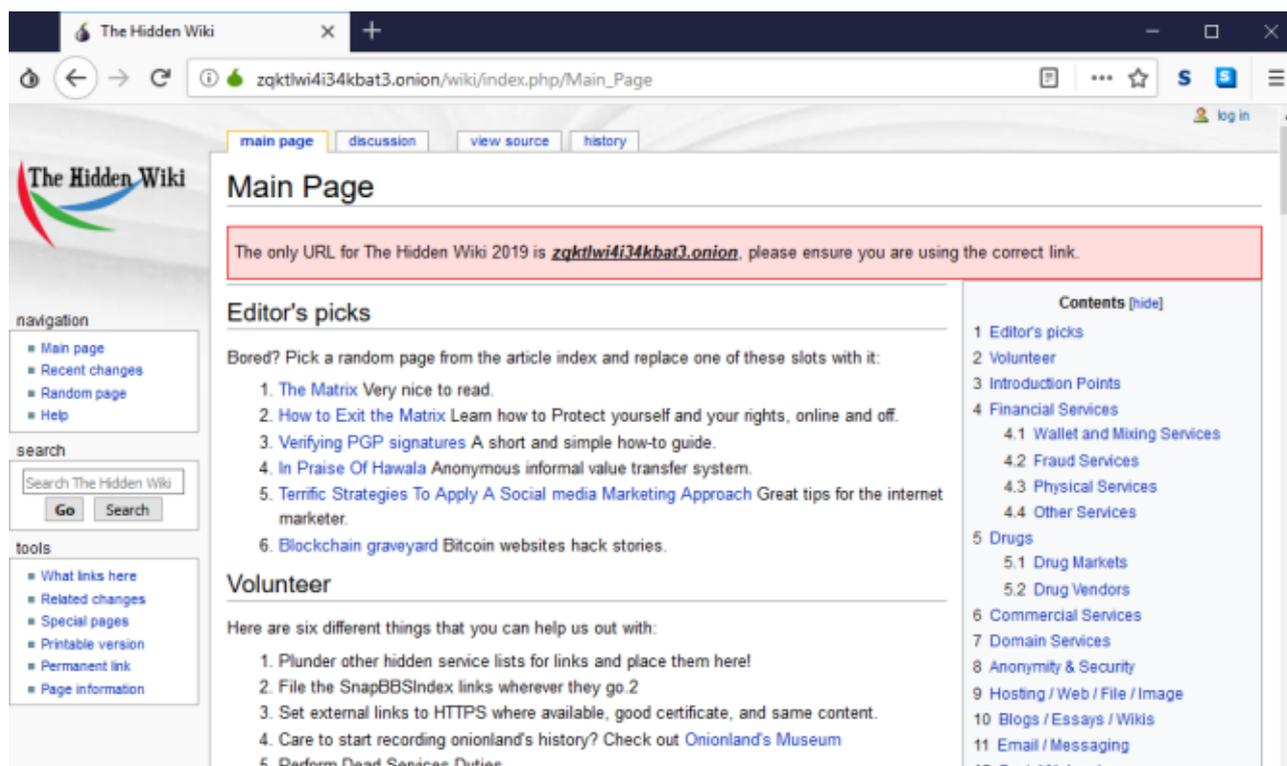
Another way you can check the Tor Browser routing is working correctly is through **whatismyipaddress**. Head to the site within the Tor Browser, and it will tell you your current IP address, as well as if that IP address is a Tor Exit Node (which is what you want).

My IP Address Is:

IPv6: 2620:132:300c:c01d:0:0:0:a

IPv4: Not detected

My IP Information:

ISP: Hextet Systems
Services: Suspected Network Sharing Device
City: Koroška Bela
Region: Jesenice
Country: Slovenia

Make My IP Address Private

Click Here

Click for more details
about 2620:132:300c:c01d:0:0:0:a
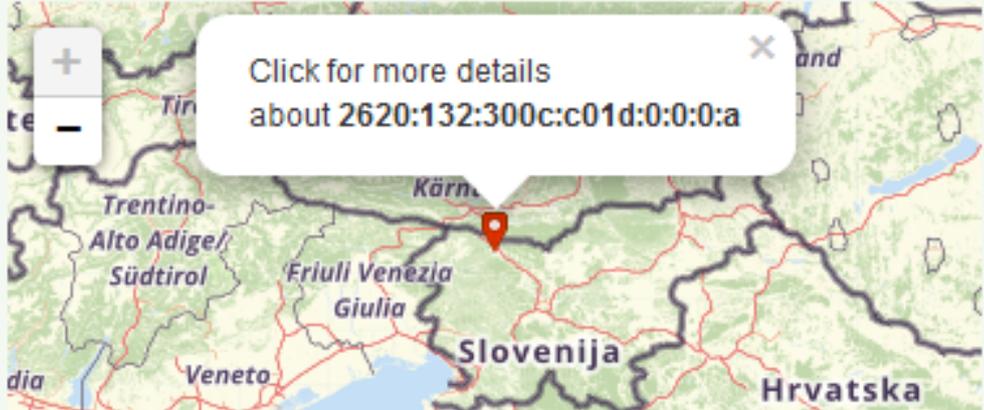
Also, check out these **tips for boosting your security while using Tor Browser**.

Four Tor Alternatives

Tor Browser isn't the only way you can access the dark web. There are several alternatives, each with pros and cons.

1. I2P

I2P is a Tor alternative that uses a modified onion routing protocol known as garlic routing. You cannot access onion sites from I2P, though like Tor, I2P is an encrypted overlay network (albeit substantially smaller than Tor).

I2P also has very few exit nodes to the clearnet, and those that do exist are rarely used. This is a slight inconvenience, but it does increase your security and privacy. Furthermore, I2P is designed for hidden sites and services from the ground up, further enhancing network security.

2. Freenet

Freenet is a peer-to-peer network, which uses a similar architecture to I2P. Again, you cannot visit onion sites with Freenet. This network allows you to anonymously share files, send messages, and publish and host anonymous websites.

In comparison to Tor, Freenet has a stronger focus on direct file sharing, using extremely powerful encryption. It is also one of the easiest networks to set up and comes with several handy directories to help you find your way about, although it is extremely slow.

3. GNUnet

GNUnet uses a decentralized peer-to-peer network to provide a secure and anonymous dark web and Tor alternative. GNUnet is a mesh network that enables randomized data routing while offering encryption, integrated electronic payment systems, decentralized social networking (known as secushare), and more.

GNUnet can access some Tor hidden services using certain configurations.

4. ZeroNet
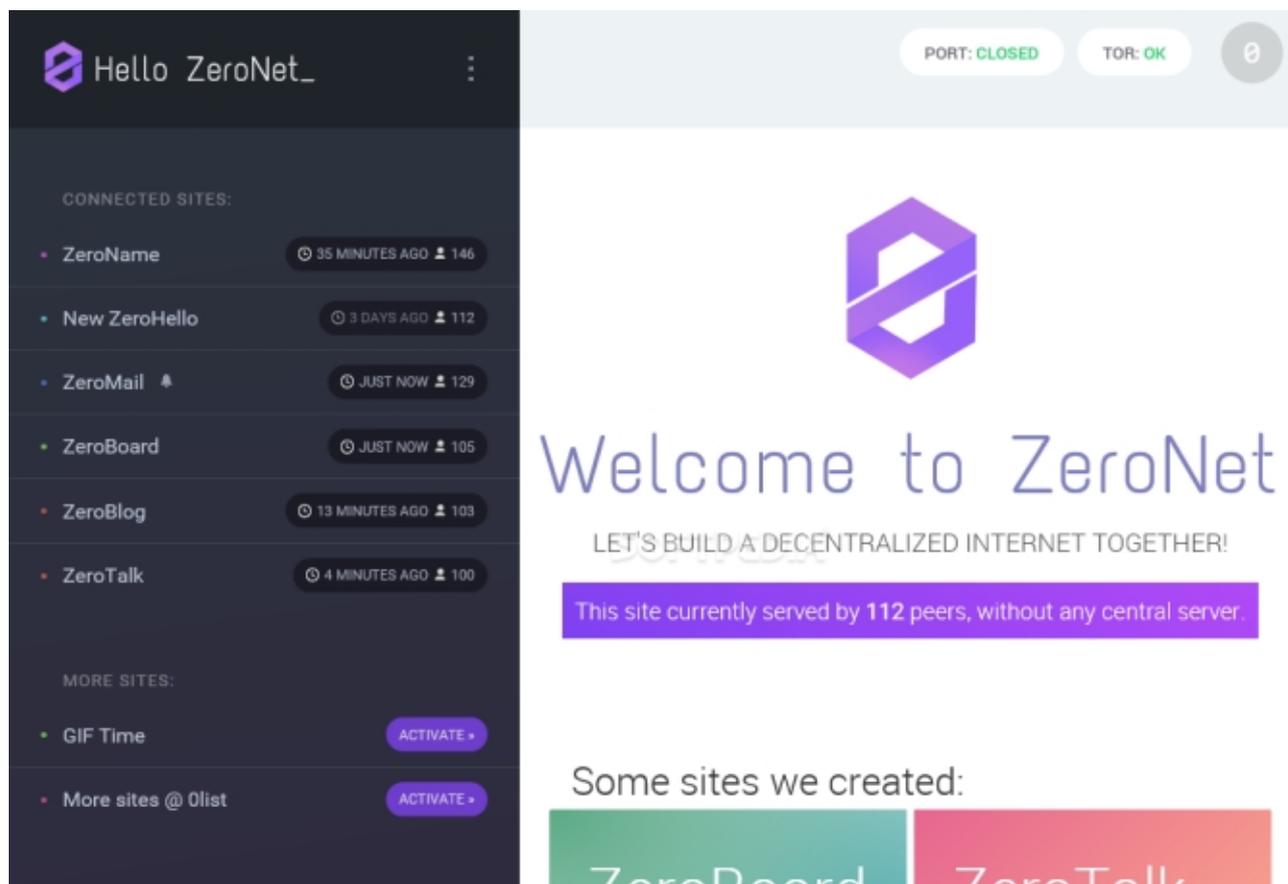
For some, ZeroNet is the evolution of the Tor network, at times dubbed "dark web 2.0.", and it's well worth your time. That is because ZeroNet is a decentralized peer-to-peer network that uses Bitcoin addresses instead of IP addresses to locate and host websites (known as "zites").

ZeroNet uses peer-to-peer technology to maintain privacy while keeping sites online. A ZeroNet zite that still has an active connection cannot be removed from the network, thus making it impossible for some censorship methods to disrupt the network. ZeroNet can access some Tor hidden services using certain configurations.

MakeUseOf's Dan Price lists **several more Tor and Tor Browser alternatives**, for different operating systems too.

You Are on the Dark Web!

But remember: Watch out for links, don't click without thinking, and don't trust anything.

Before the next lesson, please:

‣   Download and install Tor.

‣   Read **MakeUseOf Unofficial User's Guide to Tor**.

‣   Think about your security while browsing the dark web.

Don't worry about reading the whole Unofficial User's Guide to Tor. However, it does contain a lot of useful information and answers to questions you might have after this lesson.

In the next lesson: Discover dark web search engines, the best sites and services on the dark web, and more dark web navigation tips.

Lesson 5 - Navigating the Dark Web

Navigating the dark web is strange because you cannot just Google what you want. While there are dark web search engines, they're not the same as Google or other regular internet search sites. That's because the dark web isn't indexed in the same way.

In this lesson, we'll explore dark web search engines, alternative ways to browse the dark web, and cap it off with some useful dark web sites and services for you to check out.

Navigating the Dark Web in Tor

The Tor network has a few handy navigation resources that make finding other onion sites easier. As ever, be careful what you click!

1. The Hidden Wiki
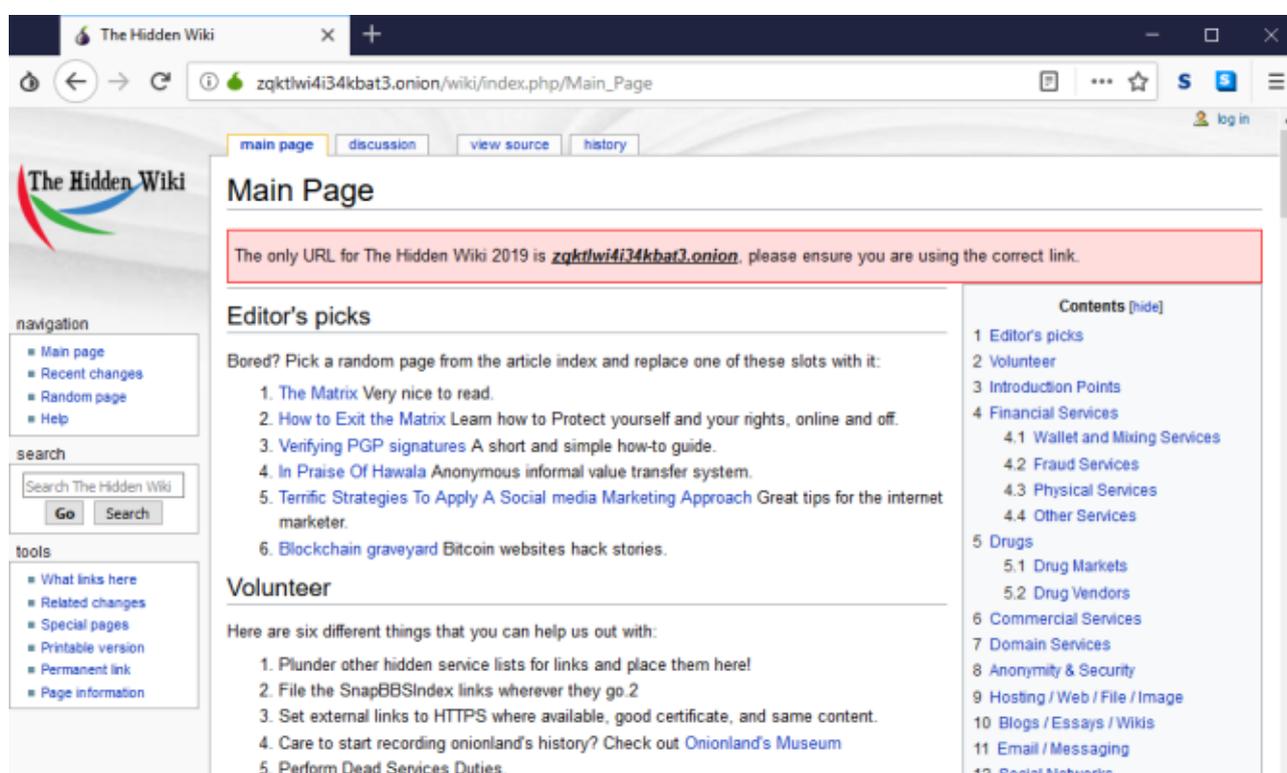
The first place to check out is The Hidden Wiki. You visited The Hidden Wiki in Lesson 4 of the course to test if your Tor Browser configuration was up and running. But it remains a handy jumping off point for new dark web users.

2. Not Evil

not Evil

hss3uro2hsxfogfq.onion

the hidden wiki   Search

query   all ◉ titles ○ urls ○

About 14636 results (827ms), now you can chat to humans or chat to ned about your query

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

The Hidden Wiki:About - **The Hidden Wiki**

[community] [report: abuse clone cp bestof]

http://zqktlwi4fecvo6ri.onion/wiki/The_Hidden_Wiki:About

Official site of The Hidden Wiki

Last Response: Tue, 23 Apr 2019 04:00:00 +0000, Ping (sec): 6.56

...h...Retrieved from " http://zqktlwi4fecvo6ri.onion /wiki/index.php?title=The_Hidden_Wiki:About&oldid=469210 "...Navigation menu...Views...Project page...Discussion...View source...History...Personal tools

Not Evil works more like a regular internet search and is the successor to TorSearch (another Tor search engine) and the Evil Wiki (another listing site).

For instance, a search for "Facebook" returns the official Facebook onion site. A search for "Proton" returns the official ProtonMail onion site, and so on.

3. Daniel's Onion Link List Raspberry Pi Directory

Daniel's Onion Link List popped up in Lesson 4. It is back again here because it is a great index directory that gives you a brief site description, the last seen and last tested dates, as well as when the onion site first hit the Tor network. Daniel's Onion Link List does include every type of site, so carefully read descriptions before hitting links. Handily, the directory also slaps a "SCAM" label on any sites that will attempt to steal your information.

The Best Sites and Services on the Dark Web

Instead of meandering through the dark web, why not use one of the following links to some of the best sites and services?
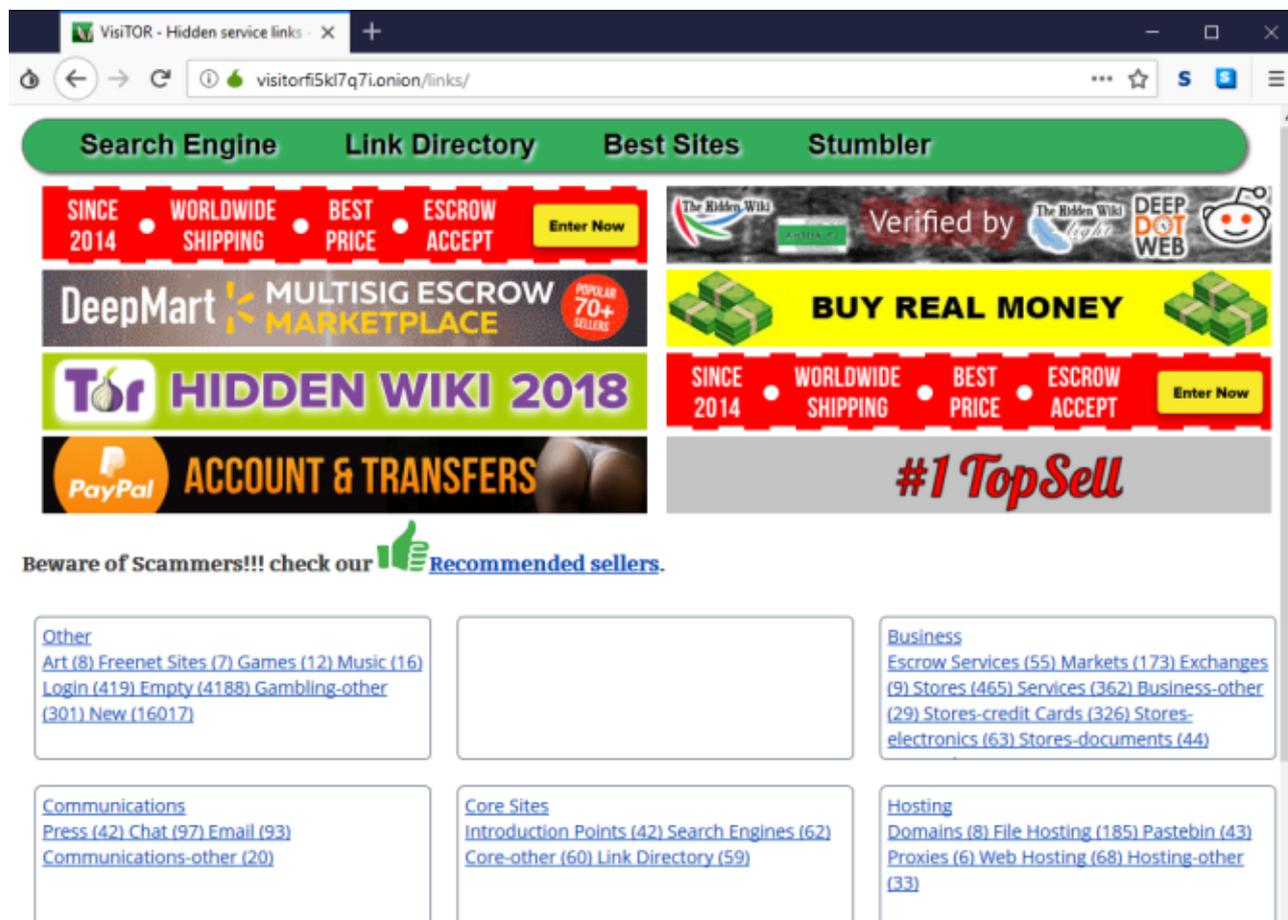
1. ProtonMail

ProtonMail is one of the best secure email services on both the clearnet and the dark web. You don't have to access the ProtonMail website using the dark web. But if you sign up via the dark web and use cryptocurrency to purchase your account, you will remain completely anonymous.

Note that ProtonMail does not and cannot access your account. It does have an automated password and username recovery service though, which is quite handy.

Also, you must create your free ProtonMail account, and **upgrade to a Premium account using Bitcoin afterwards**.

2. Visit Tor

Visit Tor is a huge directory containing links for many thousands of onion sites. There are handy sections for all manner of sites and services, including Games, Communications, Core Sites, Hosting, Politics and Religion, and so on.

Visit Tor also features a Stumble button. **Beware!** This takes you to any of the listings, **regardless of content or legality**.

3. Numbers Station

The Numbers Station is thought to link to Chinese intelligence.

The original Numbers Stations were radio broadcasts containing seemingly unintelligible sequences of numbers, words, or sounds. While it is speculation, numbers stations are strongly suspected to have links to various intelligence agencies around the globe, communicating with spies in the field.

There's not much to it, but the consistency and longevity of the site does make it somewhat unnerving.

4. The Matrix Game
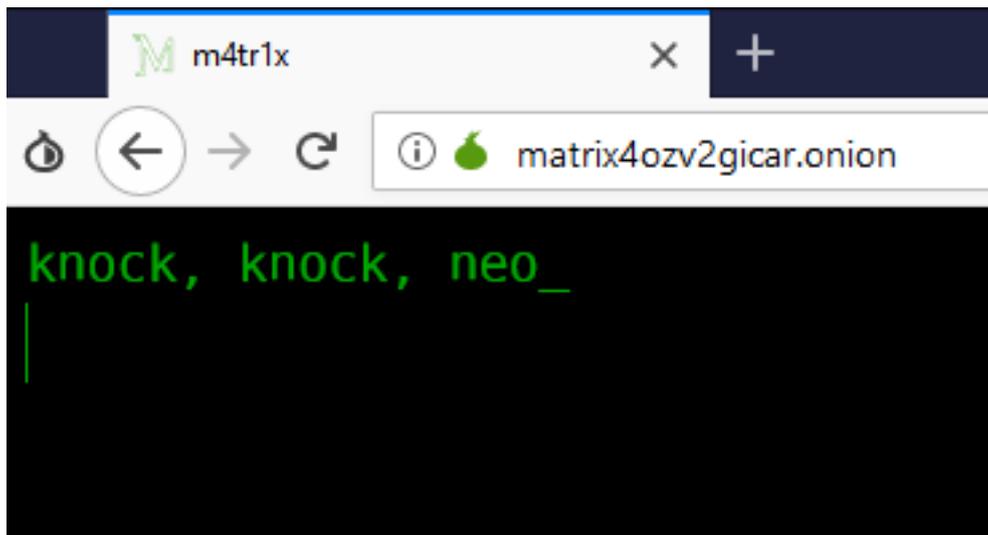
You can pretend you are Neo, straight out of The Matrix into your screen, with green text on a black background. I won't give you many details because it is a game of sorts. But if you're stuck to begin with, type "help."

5. ProPublica

The aforementioned award-winning investigative news outlet hosts a dark web version of the site. Why not just use the clearnet version? In some countries, publications like ProPublica are heavily censored due to their knack for uncovering extremely compromising information on governments, businesses, charities, individuals, and more.

The dark web version of the site also features a secure drop box for activists, whistle-blowers, and other confidential data drops.

If you encounter a cross-site scripting attack, select **Block**. This is a false positive.

6. Deep Web Radio

The dark web wouldn't be complete without a soundtrack. Check out Deep Web Radio for the sounds of the dark web. Deep Web Radio lets you stream a number of radio stations completely anonymously, without advertising, for as long as you want. There's a decent number of stations to choose from, too.

What Are You Looking For?

If you have a clear idea of what you want to find on the dark web, or use the dark web for, you can use one of the dark web search engines or directories to find what you need. The key thing to remember is that a dark web search engine doesn't work in the same manner as a clearnet search engine because of the lack of indexing. (Here is **how search engines and indexing work on the clearnet**.)

As you can see in the TORCH example, a search for Facebook doesn't return the regular Facebook page, or even the Facebook onion site. In that, be careful what you click—you can use Daniel's Link List to figure out if a link is safe or not.

Before the next lesson, please:

▸ Use one of the dark web search engines or directories to find a new onion site.

▸ Figure out your favorite dark web sites and services.

In the next lesson: A recap of what was covered in each lesson along with important links.

Lesson 6 - The Roundup

Welcome to Lesson 6 of your free MakeUseOf Introduction to the Deep and Dark Web guide. The past five lessons have covered what the deep and dark web is, how you access it, if it is legal, and how to stay secure.

This section is your guide roundup. It contains a little snippet of what was covered in each lesson, plus every link for every bit of information you could need. Plus, you'll find a few more interesting bits that will help you as you travel through the dark web unassisted.

Lesson 1: What Is the Deep and Dark Web?

Lesson 1 was your introduction to the deep and dark web, exploring the differences between the deep web and the dark web, and how the dark web works. One of the biggest things to remember from Lesson 1 is that the deep web and the dark web are different, and although sometimes people use the names interchangeably, it isn't correct to do so.

Here are the most important links for you to follow up from Lesson 1:

▸ **US Citizen Voter Records Hacked and Now For Sale on the Dark Web**

▸ **10 Search Engines to Explore the Invisible Web**

Lesson 2: Why Would You Access the Dark Web?

Lesson 2 of the guide was a look at accessing the dark web: how do you get onto the dark web? Furthermore, once you know how to access it, is it even safe to do so? Lesson 2 also considered the legality of the dark web and the content you can access, as well as what you can do once you access it.

Here are the most important links for you to follow from Lesson 2:

▸ **Avoiding Internet Surveillance: The Complete Guide**

▸ **How to Bypass Web Filtering and Censorship**

▸ **5 Reasons to Upgrade to Malwarebytes Premium**

Lesson 3: Accessing the Dark Web Using Tor

This was the big lesson. You finally accessed the dark web using Tor Browser. Lesson 3 included information on how you download the Tor Browser, install it, and then complete its configuration before accessing the dark web for the first time. Remember: make sure you update Tor Browser before hitting the dark web — an out-of-date Tor Browser can expose your data!

Here are the most important links for you to follow up from Lesson 3:

▸ **How to Set Up a VPN in Windows 10**

▸ **How to Set Up a VPN on Your Mac**

▸ **Everything Linux Users Need to Know About Installing a VPN**

▸ **How to Set Up a VPN on Android**

Lesson 4: Using the Dark Web Securely

Lesson 4 covered dark web security. The dark web certainly has some nefarious sites and services, but you don't have to click those links. Lesson 4 also showed you how to install a VPN on the most common operating systems, as well as the Raspberry Pi and a host of routers.

Something else to consider from Lesson 4 was using Bitcoin to make purchases on the dark web. Remember, criminals operate on the dark web and you should take proper precautions to isolate yourself.

Here are the most important links for you to follow up from Lesson 4:

▶ **5 Ways to Stay Safe From Bad Tor Exit Nodes**

▶ **7 Tips for Using the Tor Browser Safely**

▶ **The Best Dark Web Browser Alternatives**

▶ **The MakeUseOf Unofficial User's Guide to Tor**

Lesson 5: Navigating the Dark Web

Lesson 5 was your guide to navigating the dark web. Even though the dark web is microscopic in comparison to the clearnet, you don't have the use of common internet search tools. Thus, you need to know either exactly what you are looking for, or an alternative method for finding the deep web sites you want.

Here is the most important link for you to follow up from Lesson 5:

How Do Search Engines Work?

Guide Complete: You Can Explore the Dark Web

You have finished the free MakeUseOf Introduction to the Deep and Dark Web guide!

You now know the difference between the deep web and the dark web, how to access the dark web, and why you would want to do that to begin with. Better still, you know how to keep yourself and your computer secure while you explore what the dark web has to offer, as well as why using a VPN gives you an extra security boost.

Thank you for reading and learning, and be safe.