The Ultimate Guide
TOR & the Deep Dark Web
(For Beginners)

by

THOMAS CRENSHAW
Join my list here

Note: My team and I have purposely repeated certain paragraphs through out the book in order to help you to retain it – we always repeat certain things of interest that should be ingrained in your mind as the reader. Repeating certain things is done on purpose – it is not an accident.

What's Inside:

How To Safely Access The Deep Dark Webs

Accessing the deep web is easier than you might think. In fact, you probably already have. The media hasn't done a great job of differentiating what's considered the deep web and what is the dark web — two similar names for two very different things.

What Is The Deep Web?

The deep web is just like it sounds — below the surface and not completely dark.

Search engines like Google, Bing, and Yahoo are able to search and index websites because of links. They use links to rank search results according to things like relevancy, inbound links, and keywords. Regular browsers search the so-called "surface web," but that's where the search stops.

For instance, if you wanted to search a public library catalog to find a book, you couldn't type the title into your browser's search bar and expect Google to return a meaningful result for your library. That level of information would be located in the deep web.

The reason search engines can't return this data to you is because there are no links. (Search engines crawl the internet by visiting one web page, then the links on that page, and then the links on subsequent pages.)

Instead, you would have to go to the public library's website and use a search bar inside the website to locate this data on the library's servers.

This kind of information is all over the internet. Almost every time you search internally on a website, you're accessing deep web content.

What's On The Deep Web?

The deep web holds the content that's invisible to search engines. Here are a few examples of what's on the deep web:

- The content of your personal email accounts
- The content of your social media accounts
- The content of your online banking accounts
- Data that companies store on their private databases
- Content contained within scientific and academic databases
- Medical records
- Legal documents

A lot of what exists on the deep web consists of information that you probably wouldn't want to turn up in a web search — like your checking account information — because it's private and could be misused.

A rule of thumb: If you have to log in to one of your accounts by providing a user name, password, or some other type of authentication, the information you access is on the deep web.

That's a good thing. The deep web can help protect your personal information and privacy.

With Norton™ Secure VPN, check email, interact on social media and pay bills using public Wi-Fi without worrying about cybercriminals stealing your private information

Is The Deep Web Safe?

The **deep web** is a fairly safe place, especially when you compare it with the **dark web**. The dark web represents a sliver of the deep web. Dark web websites are often associated with illegal activity — but not all of them. More on that later.

Accessing content on the deep web is relatively safe. Think about it. You probably check your email and your credit card statements online without worry. But that doesn't mean that accessing that personal information has no risks.

For instance, your accounts on the deep web contain a lot of your personal information that criminals might value. That's one reason why it's important to use strong, unique passwords on all your accounts. That might include a hard-to-guess combination of letters, numbers, and symbols.

Here's another potential risk. You might be tempted to access your personal information on the deep web on an unprotected public Wi-Fi network. For instance, you might want to pay your bills while waiting to catch a flight at an airport.

But don't do it on a public network. Instead, use a virtual private network — commonly known as a VPN — which can encrypt your data and help protect your online privacy.

Here's One More Risk. It's also possible you could receive an email that appears to be from a reputable source. It might look like it's from the IRS, for instance, an agency that keeps your personal information on the deep web. The email might ask you to supply your Social Security number to access your account or to click on a link to respond to a request for information.

Don't do it. The IRS will never ask for your information through an email. That means someone is likely sending you an email to trick you into supplying valuable information. This is commonly referred to as "phishing."

While the deep web is relatively safe, it's always smart to practice safe internet habits.

What Is The Dark Web?

The dark web is a different story — and probably what you might have assumed the deep web was if you read about it in a newspaper or saw a story on TV. But remember, the deep web and the dark web are two distinctly different things.

Although these two terms have been used interchangeably, one — the deep web — contains mostly harmless data and digitized records. The other — the dark web — has raised concern worldwide about criminal activity.

Regular browsers can't access dark web websites. Instead, the dark web uses what's called The Onion Router hidden service protocol. "Tor" servers — derived from "The Onion Router" — are undetectable from search engines and offer users complete anonymity while surfing the web. At the same time, dark web website publishers are also anonymous thanks to special encryptions provided by the protocol.

When you access the dark web, you're not surfing the interconnected servers you regularly interact with. Instead, everything stays internal on the Tor network, which provides security and privacy to everyone equally.

Worth noting: Dark web website addresses end with .onion instead of the surface web's .com, .org, or .gov, for example.

What's On The Dark Web?

The dark web operates with a high degree of anonymity. It hosts harmless activities and content, as well as criminal ones.

For instance, one dark web website might provide complex riddles. Another might be a kind of book club that makes eBooks look more professional. Yet another might offer a forum for people who believe free speech is threatened.

But the dark web is better known for dark content — meaning, illegal and sometimes disturbing content. For instance, here's a sample of illegal things you can find on the dark web.

- **Stolen information.** When there's been a data breach, there's a chance the accessed information — from Social Security numbers to bank card numbers — will end up for sale on the dark web. You can also buy things like log-in credentials, hacked Netflix accounts, and more.
- **Illicit substances**. Illegal drugs — and prescription drugs — are peddled on the dark web. You might also find toxic chemicals that can cause other types of damage.
- **Disturbing and dangerous items and services.** It can get ugly fast. Things like gore, murderers-for-hire, human trafficking, child pornography, body parts, counterfeit goods, and guns for sale can be found on the dark web.

In short, you can buy just about anything you can imagine — including things you'd probably be better off not imagining.

What makes it possible to do business on the dark web? Financial transactions use Bitcoin, the cryptocurrency that helps assure buyers and sellers anonymity.

Here Are A Few Safety Issues To Consider

- **Criminal element.** There's a chance you will find websites run by criminals. Beyond selling illegal goods and services, they may seek to exploit you and steal from you.
- **Breaking the law**. You can be prosecuted for things you do on the dark web. It's important to behave in an appropriate and legal manner.
- **Suspicious links**. If you click on any links, you may be taken to material you might not want to see. It's also possible that clicking a link or downloading a file could infect your device with malware.
- **Law enforcement**. Law enforcement officials operate on the dark web to catch people engaged in criminal activity. Like others on the dark web, law enforcement can do their work under a cloak of anonymity.

If you decide to venture to the dark web, it's smart to be selective about the websites you access.

Accessing The Dark Web With Tor Browser

Getting to the dark web is actually a lot easier than you might think. All you have to do is download a dark web browser, like the Tor browser.

Once you install a dark web browser on your device, it functions just like a regular browser: type in a URL, and off you go.

However, finding the material you're looking for on the dark web is more difficult than using a search engine like Google. The dark web doesn't have an index or ranking system to help you find what you need.

There are such things as dark web search engines. One called the Uncensored Hidden Wiki offers some guidance to content on the dark web, but it may include illegal websites.

How To Safely Browse The Deep Web & Dark Web

If you browse the deep web — even if it's just to check out your dental bill — it's a good idea to equip your device with trusted security software and keep it up to date. We already talked about using a VPN on public networks.

Here are a few tips and tools to help stay safe when using Tor and other browsers. There's a lot more to consider, but this should give you an idea of some of the issues — good and bad — to consider.

- Tor is known for providing online anonymity, so it can be effective for sharing sensitive information with family or reporting corruption or abuse.
- Keep Tor and Tor applications updated. Make sure your device's operating system is also up to date.
- Don't use your regular email on websites when using Tor. While Tor is designed with anonymity in mind, providing your regular email address could expose your identity.

Browsing The Dark Web And Online Security

The presence of illegal activity calls into question the "character" of some dark web denizens. That's why it's important to take care and help protect your personal information and identity.

Poking around on the dark web is where some people get themselves into trouble. Unlike the deep web, which contains important and useful information, the dark web is riddled with illegal and unconscionable activity.

Because Tor servers keep users and publishers completely anonymous, there's no way to regulate or control the content, products, and services being offered inside the dark web. Plus, there's no way to trace communications or keep financial tabs on responsible parties because all payments are made and received using Bitcoin, a digital currency that operates independently of a central bank.

On the flip side, there are publications on the dark web that believe it's the only way to obtain and sustain a truly free press.

Before you get lost in the dark, be sure to educate yourself on the dangers of the dark web. Make sure you install and run strong security software on your computer and devices to help ensure the privacy and security of your data.

In general, don't underestimate the darkest side of the dark web. Here are a few additional things to keep in mind.

How The Dark Web Can Be Dangerous

There are people and things on the dark web that you'll want to avoid. Here are a few of them:

- **Viruses**. Some websites could infect your devices with viruses, and there are a lot of different types of viruses to watch out for. Remember to never download anything from websites you don't trust.
- **Hackers**. You can find hacker forums on the dark web. You can hire computer hackers to do illegal activities. Not surprisingly, a lot of these people would be willing to hack your devices.
- **Webcam hijacking**. A website on the dark web may try to get a remote administration tool — also known as a "RAT" — onto your device. That can lead to someone hijacking your webcam — essentially, letting them see what you're up to through your device's camera lens. It's a smart practice to cover your webcam with a piece of paper or tape if you're not using it.

Dark Web Content May Be Illegal

Anytime you're in the company of illegal drugs, illegal content, and other sordid online activities, you could risk landing in legal trouble.

A mistaken keystroke or simple curiosity might not be a reliable defense. Here are two examples of dark web content and activities that would raise legal concerns.

- Sharing pictures and videos of child pornography. In one FBI arrest, the perpetrator traded material on a website with more than 100,000 registered users. The FBI busted him.
- Purchasing illegal goods or services. If you buy illegal drugs or hire a hit man, you can be arrested for committing an illegal act. But browsing a website that offers those two things would not be illegal.

Dos And Don’ts On The Dark Web

Law enforcement officials have an interest in stopping illegal activity on the dark web. When they do, there are legal consequences.

Here are some notable cases where law enforcement took down criminals doing business on the dark web.

Silk Road. This online black market sold illegal drugs. It was launched in 2011. Total revenue was estimated at US$1.2 billion. Founder Ross Ulbricht was convicted and sentenced to life in prison.

AlphaBay. This was another online black market, launched in 2014. It grew to an estimated 10 times the size of Silk Road. Merchandise ranged from drugs to breached data. Alleged founder Alexander Cazes was arrested. He was found dead in a Thai jail cell, apparently by suicide, several days later.

Hansa. This online black market expanded after AlphaBay was shut down and vendors moved to the platform. But Dutch police had already infiltrated the marketplace and seized information tied to its operation. Police shut down Hansa in 2017.

Why Does The Deep Web & The Dark Web Exist?

The deep web and the dark web both offer a degree of privacy and anonymity.

The deep web helps protect your personal information that you probably want to stay private. But if you access your bank account, it's not entirely private. The bank knows you've accessed your account.

The dark web operates on the principle of total anonymity. What you do there is your business. With certain precautions, what you do there can't be tracked or traced to you.

For some people, privacy is a big concern on the internet. They might want control over the personal information that standard internet service providers and websites collect on them.

Freedom of speech also is an issue, and some people would make an argument for privacy and anonymity based on the First Amendment. That's one reason why law-abiding citizens might value the privacy of Tor and other dark web browsers.

Anonymity can have positive effects — like being able to express views that are unpopular, but not illegal. And the dark web helps make things like that possible.

Are You Wanting To FIND Deep Websites – This Is How You Do It.

Today, I am going to share all possible ways to find the deep web sites so that you can easily find out any deep web service anonymous tor links and get into the deep web.

What are the Deep Web Sites?

Deep Web sites are those websites on The Tor network which can't be indexed by traditional search engines like Google, Yahoo and Bing and only

accessed with help of special configured software like Tor Browser. Deep web/Dark web website ends with .onion extension for example http://xyz1234aabc.onion.

Deep Web Websites name are not memorable since they are quite long and their charters are also random. Legal and illegal both type websites are exist on the dark net.

Deep Web sites are mainly designed to offer service anonymously without getting too much attention. One major issue with websites on the deep web is they go offline often. Sometimes they back online after 2 -3 days or some time goes for forever. But when you know how to find a deep web/tor site, you need to worry about such issues.

Now I think you know what are deep web sites? It is time to move towards next section.

Why It Is Hard To Find A Deep Web Site?

As I earlier said a deep web website can't indexed by normal search engine. That's why you can't Google them. So you need to know about special search engines known as deep web/dark web search engines or Tor Directory. Some

Clearnet websites are also sharing deep web links but only few are able to provide working sites links. Most of websites have dead links as I said recently onion sites go down often. That's why finding the deep web websites become harder for users who don't have much technical knowledge. But don't worry by sharing this article, I made you task easy whether you are techy or not.

Tools You Need for Finding Deep Web Sites

I think you have already know that you need some special tools to find the deep web sites or anything on the darknet. Three main tools are Tor Browser, VPN Software and Dark Web/Deep Web Search Engines.

Tor Browser

Tor Browser is one of the most used deep web browsers to access Tor websites/deep web websites. It is completely free and provides facility for anonymous browsing and prevents monitoring of internet activists. Tor Browse directs traffic through an overlay network of seven thousands plus relays to hide user's real location and activities.

When you access Clearnet websites like Google.com, Facebook.com and any other websites which you can Google then you need an Internet browser like Google Chrome, Mozilla Firefox and Safari etc. Same now you need Tor Browser to access deep web or even finding deep web sites also.

Recently I wrote Tor Browser Review, where I covered all things like is Tor Browser safe enough to browse dark web, is it illegal or how to use Tor Browser. I think you should check this for better understanding of Tor.

VPN Software

When Deep Web Word comes into my mind, Very first thing which got my attention, my own security. I always ask myself, am I completely secure and fully anonymous? Yes, you should also ask yourself.

You can't put yourself in danger whether you are learning about deep web/dark web or accessing darknet. Always make sure to run your VPN software first of all then start browsing, learning about deep web or anything what you are doing. It makes you 100% secure and anonymous by adding additional anonymity layer.

There are lots of VPN Services available in Industry. So Choosing best is become a tedious job. That's why recently I tested several VPNs and finally compiled a list of top 10 VPN services. Here you can have a look at this list.

NordVPN is suggested.

How to Find Deep Web Sites

Let me talk about possible easy ways to find out any hidden service link on the deep web/darknet. Some of most commonly used ways are deep web search engines, onion directory, Reddit. Let me dig deep.

Onion Links Directory plus Blog

Link: https://www.thedarkweblinks.com/
This is the best place where you can get active deep web sites links for all categories including carding, paypal, torrent, social networks, red room, erotic and many more.

Best thing about TheDarkWebLinks.com, it gives you detailed and informative description means you can know what a particular tor website is offering to their users. Are you wondering? How I am sure that all websites links are active.

Let me tell you my friend, this tor directory list is managed by me and every week, I check this list to make sure all mentioned onion links is working. And add to new coming hidden service links also here. I am quite sure once you check this dark web sites directory; you will never look further for any other place. In case, you are not satisfied with

TheDarkWebLinks.com then you need to take a look at second solution to know how to find deep web sites.

Deep Web Search Engines

Deep Web Search Engines are those search engines which are capable to index .onion urls and provide several relevant results of your deep web search query. Yes, they are simple and easy to use like Normal search engine Google, Yahoo and Bing.

They offer you full privacy; they don't keep any eye on your browsing history they don't track your searches as normal browser do. There are many users who use Duckduckgo to browse Clearnet also since they care more about their privacy.

To search anything on the deep web/dark web, you need Tor search engines. Here, I am listing some simple and easy to use Search Engine links so that you can easily find deep web sites in seconds. Don't worry, I will also explain how to perform deep web search with the help of onion search engines.

1). Duck Duck Go

Onion URL: http://3g2upl4pq6kufc4m.onion/

2). Torch

Onion URL: http://xmh57jrzrnw6insl.onion/

3). Ahmia

Onion URL: http://msydqstlz2kzerdg.onion/

4). NotEvil

Onion URL: http://hss3uro2hsxfogfq.onion/

5). Candle

Onion URL: http://gjobqjj7wyczbqie.onion/

So these are best and working Tor search engine links. They are active from a very long time and give you good relevant results for your searches. You can take a look at my recent post about Deep Web Search Engines to know detailed info about these.

How to Search the Deep Web with Tor Search Engine

Here is how to find deep web sites or how to search the deep web using any Tor Search Engine. Here, to explain all steps, I am using Ahmia. Follow below steps to get started and find out results of your queries.

1).Run your VPN Software ->> Connect with Onion over Server

2). Launch Your Tor Browser (Make sure you have got new IP address with the help of VPN before following second step) & Disable java Script, you can do this simple click on S! Symbol.

3). Copy Ahmia Onion link (http://msydqstlz2kzerdg.onion/) and paste into the Tor Browser and hit enter button. Now will get a window like below.

4). Now type your search query into search box and you will get result with deep web site name, onion link and nice description (Enough to understand website service).

5). Now you can click any of link and you have got what you are looking.

Now you can search anything on the deep web and find deep web sites/tor links easily less than one minute. You can use same process with other dark search engines to find anything on darknet. But in case if you are not able to find what you want with the help of search engine and tor directories. Then you can give a try to Reddit.

Reddit

Here is how to search the deep web links/darknet links with the help of Reddit. Reddit is known as the front page of Index. Here you can find most interesting content of related to any category. Same applies for the term Deep Web. Simply type your query into search box and hit enter, you will get all relevant subreddits list in front of you like below screen.

Click at any Subreddit link, which you find most relevant to your search query. Even you can subscribe these subreddit also.

Searching anything and finding interesting at Reddit is very easy due to its Upvote system. They keep most interesting content up and less interesting content down according to user engagement and interest. I think everyone can easily find deep web sites with the help of Reddit by just exploring Deep Web Subreddit.

Popular deep web /dark net subreddit for your convenience.

- https://www.reddit.com/r/onions/
- https://www.reddit.com/r/deepweb/
- https://www.reddit.com/r/DarkWebLinks/
- https://www.reddit.com/r/darknet/
- https://www.reddit.com/r/TOR/

NOTE: You have just now learned many of the possible ways to find deep web sites. These lessons have explained exactly how to search the deep web.

How to Hop on the Dark Web – Step by Step

Dark web, deep web, clear web – just words or more? Many people are interested in learning how to the darkness of the Internet. This guide is meant for you. If you want to learn all about Tor Onion, Silk Road, secret, hush-hush Governmental ops, and how to get on the dark web you came to the right place.

What is the dark web anyway?

The differences between the deep web, dark web, and clear net. The clear web is the very first and very visible layer of the Internet. Basically, it's what we see when we do a Google or Bing search for things like cat videos or popular YouTube songs.

From a technical standpoint, clear web defines the content that it's indexed, crawled, and displayed by the various search engines. Unfortunately, the clear web accounts for ***approximately 4 percent of the Internet***. So, if the clear web is only a very tiny portion of the Internet, what happened to the rest?

Thor Foresight provides: Automatic and silent software updatesSmart protection against malwareCompatibility with any traditional antivirus.

Secure Your Online Browsing!

Deep Web Vs. Dark Web

Welcome to the deep web, the part of the Internet that's not indexed by search engines. There's nothing spooky about the deep web; it contains stuff like scientific white papers, medical records, tax-related info, PayPal subscriptions, army communique, and much more. Although the deep web's

hiding behind HTTPS forms, its contents can be accessed if you know what you're looking for.

Most of the websites hosted on the dark web can be accessed on a credential basis. For instance, if your health provider has a website capable of displaying bloodwork tests online, that particular section will be hosted on the deep web – it will not be indexed by Google or Bing and can only be accessed via password.

The Deep Web Accounts For About 90 Percent Of All Internet.

Remember: **Clear, Deep,** and **Dark**.

What's the dark web? Well, if the clear web is Google's BFF and the deep web, its secret lover, then the dark web can only be the evil twin or the oddball.

Accounting for **6 percent of the Internet**, the dark web is a most peculiar blend – on the one hand, it's a cesspool, a rendezvous place for drug dealers, black hat hackers, hitmen, and human traffickers. This Internet fold acts like a liaison between political outcasts and people the free world. It's also used by people who want to submit anonymous tips (whistleblowers).

The dark web is favored by both groups because of its ability to render anyone and anything invisible. Privacy and anonymity are what you might consider the core values of the darknet. There's no such thing as a mother-server that hosts the entire dark web, but rather a swarm of servers and nodes that can only be accessed through onion-type links.

So, what are those?

More on Tor Onions

Since everything's decentralized on the dark web, there are no crawlers to bring together the information. Even the URLs, if we can call them that, are infinitely different from what we're used to.

For instance, if you want to access a site like YouTube, all you need to do is to write the URL in the address bar or search for the website using google.com.

Now, on the dark web, you'll have to know the URL right to the last decimal and character to access it. All dark web addresses contain seemingly random strings comprised of numbers and letters, followed by a .onion extension.

Again, we shouldn't lose sight of the fact that the dark web's the place where the bulk of criminal activities take place. Everything little sordid detail you heard over the news about the dark web is painfully true.

This is the place where hackers come to purchase data stolen from users or companies or offer their services in exchange for Bitcoins or other forms of cryptocurrency. If you dare to dig deep enough, you can uncover other hair-raising activities such as human trafficking, child pornography, torture, or murder on demand.

#1. Install a VPN

VPN services are a must when you're attempting to access the dark web. Why? Because of the long arm of the law, of course. Technically, you are free to surf on this Internet layer, provided that you don't engage in any illegal activities. However, even if you're only casually browsing the darknet can could be investigated – but searching on the deep web is NOT illegal.

This means that if the authorities would intercept your darknet connection request, they would have had enough reason to search your house and confiscate the machine used for browsing. So, do yourself a favor and download a VPN before messing about on the dark web. Need a hand picking VPN?

#2. Install an adequate browser

The first rule of the dark web – never, ever use your default browser to search for stuff on the darknet. Popular browsers like Chrome, Opera, or Firefox

have tracking technologies that make you very visible on the authorities' radar. Many people download Tor, which is, by far, the safest and easy-to-use onion browser.

Of course, there are others who would argue that Tor being made by the military for covert communication makes it unreliable, privacy-wise since it's believed to be watched. I wouldn't take that one for granted, but, then again, there's no smoke without fire. It's all up to you.

Tor, VPNs And Other Demons

Anyway, going back to Tor – why use this particular browser over a regular one? A regular browser mediates between the user's search request and the site about to be accessed. Normally, your query will go through the ISP's DNS, which in turn consults other resources to help you get the answer you were looking for.

With Tor, the search request kind of bounces around multiple Tor relays before completing your search request. You're probably wondering about what the heck are Tor relays. The web is nothing but a conglomerate of servers, which are managed either by companies or on volunteer-basis.

The same principle applies more or less to what we call the dark web. Since it's the dark side of the Internet we're dealing with here, secrecy and untraceability become inherent. Thus, the info's stored on Tor relays which are managed by volunteers.

So**, what happens when you want to access a dark web onion?** First of all, if you followed my advice and installed a VPN, the tunneling signal will be encrypted. This means that your ISP won't have a clue about what you're about to search for. Sure, it can still see that you want to access a Tor node, but other than it's blinder than a mole.

From there, it will be redirected to another node and then another one. Why does it do that? For anonymity reasons, of course; 'no breadcrumbs' means that there's no way for someone to trace the signal back to you.

VPN Only?

There are a couple of more precautions you must take before you can pop open Pandora's box of dark Internet wonders. Getting back to Tor and VPN. There's no broad consensus on dark web safety.

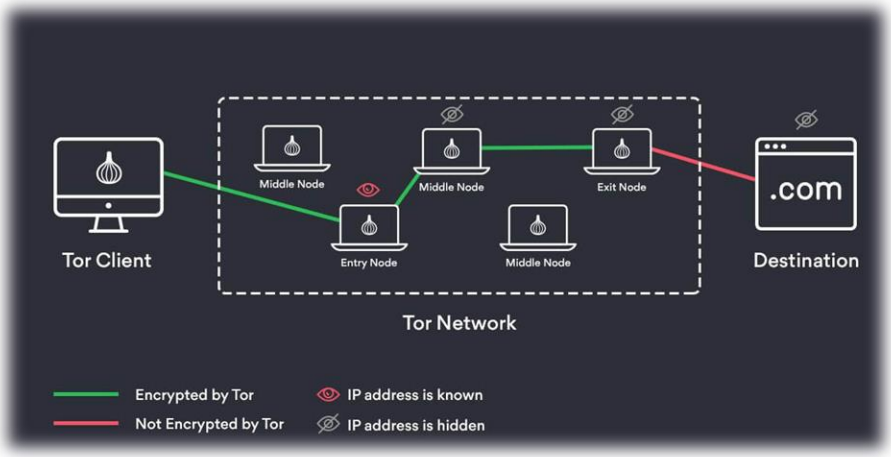
However, everyone tends to agree that using only Tor is not enough. The two of them (Tor and VPN) work in tandem and, as it happens, there are several ways of tunneling your way all the way through the dark web using this dynamic duo. Here's what you need to know.

METHOD I – TOR OVER VPN

Sounds very techie, doesn't it? Well, it's really not that complicated – using the Tor over VPN method means connecting to a VPN service before using the Tor browser. Have to say that this is the most popular and safest method to access onion links, and, on my part, a marriage made in Heaven: Tor's an excellent 'anonymizer', while VPN safeguards your privacy.

When using this method, Tor will encrypt your request, which will pass through your ISP unhindered. From there, it will go through a VPN server that conceals your IP and wipes geo-locations tags and other elements your Government or ISP might use to track the request.

Next step – your request will be transferred to Tor entry nod which in turn transfers to one or more Tor relays. From there, it gets slingshot to several Tor exit nodes. Afterwards, your request will be matched with the appropriate website. Tricky, but effective; that's why it's, by far, the best method to access dark web content.



***PROS OF USING TOR OVER VPN*:**

- Session logs are not stored (metadata, IP address).
- Traffic's completely encrypted.

***CON(S)*:**

- It doesn't offer protection against malicious Tor exit nodes.

Method Ii – Vpn Over Tor

Not very safe, but it's still useable. Recall how Tor oven VPN works? Well, VPN over Tor is basically its opposite – instead of going through the VPN first, the signal passes through the Tor network, before going through the VPN. Why is this method so unpopular? Because it's not as safe as Tor over VPN.

If the signal goes through the Tor network first, your ISP will be able to see that you are attempting to connect to a Tor node. Though no one should bat an eye just because you're attempting to access the dark web, keep in mind that in some countries, like the United States, even a simple foray can get you in trouble.

Pro(S) Of Using Vpn Over Tor:

- Great if you trust your ISP, but not the VPN provider.
- Can bypass blocked Tor nodes.

CON(S):

- ISP can see you trying to access onion content.
- Susceptible to end-to-end timing attacks.

If you want to see what lurks in the dark corners of the Internet but don't really trust Tor, there are alternatives. Here are a few:

1. **I2P** – great privacy protection and can access hidden onion links.
2. **Matrix.org** – an open-source project just like Tor. Great for IoT data transfers, chats, and WebRTC signaling.
3. **Orbot** – basically a Tor for Android.
4. **Globus Secure Browser** – paid Tor alternative. VPN-powered. It allows the users to select preferred geolocation. If you want to take it for a spin, Globus features a five-day trial period.
5. **Comodo Ice Dragon** – Firefox offspin. Employs multiple malware safeguards. Open-source project.
6. **FreeNet** – open-source project. Sports the Darknet and OpenNet anonymous browsing technologies.

#3. Install a VM or disposable OS

I strongly recommend surfing on the dark web using virtual machine software instead of your locally installed Windows. Why? Because it's easier to contain malware in a virtual environment, which can be fully controlled.

It's like in those movies where the doctors are experimenting on deadly viral strains from behind the safety of a glass enclosure. Now, if you really want to take the physical storage devices out of the equation, you can use what I like

to call a disposable operating system – easy to deploy and to get rid of if you by chance you run into any trouble. All you'll need is an 8GB thumb drive, an installation package, and a couple of minutes to get things up and running.

How To Install Tails Os

Source: TechSpot

Step 1. Get yourself a thumb drive; 8GB will do, but you can buy one with more space if you plan on using it for anything else. Nothing will happen to the stick (probably).

Step 2. Hop on the web and download the **installation package for Tails OS**.

Note: Tails is a Linux-based live operating system which can be booted from a USB stick or DVD. I recommend using a stick since DVDs have a read-only function after you're done burning well and accessing the dark web required a bit of writing.

Chill, because nobody will ever find a record of you ever fiddling around the darknet. Note that Tails' installation package is the .img format, which means that you'll need software capable of burning images on your thumb drive.

My recommendation is Universal USB Installer, which is very intuitive. You can also go along with Rufus. The choice is yours. For this tutorial, I've used Universal.

Step 3. Insert the stick and do a quick format. Be sure to use FAT32 to root out any compatibility issues. It shouldn't take longer than a few seconds.

Step 4. Download and install **Universal USB Installer** or **Rufus**.

Step 5. Fire up Universal USB or Rufus.

Step 6. Under "*Step 1: Select a Linux Distribution from the dropdown to put on your USB*" select **Tails**.

Step 7. Under "*Step 2: Select your ubuntu*desktop*.iso*", click on the browse button and select the downloaded Tails .img file.

Step 8. Under "*Step 3: Select your USB Flash Drive Letter Only*", use the dropdown box to select your thumb drive's letter. If it doesn't show up, check the "now showing all drives" option.

Step 9. Review the info and hit **Create** when you're done.

Note that the *process can take anywhere from 5 to 30 minutes* depending on your machine. Sit back, relax, and wait until the installation's done. When you're ready, hit the Close button and you're all set.

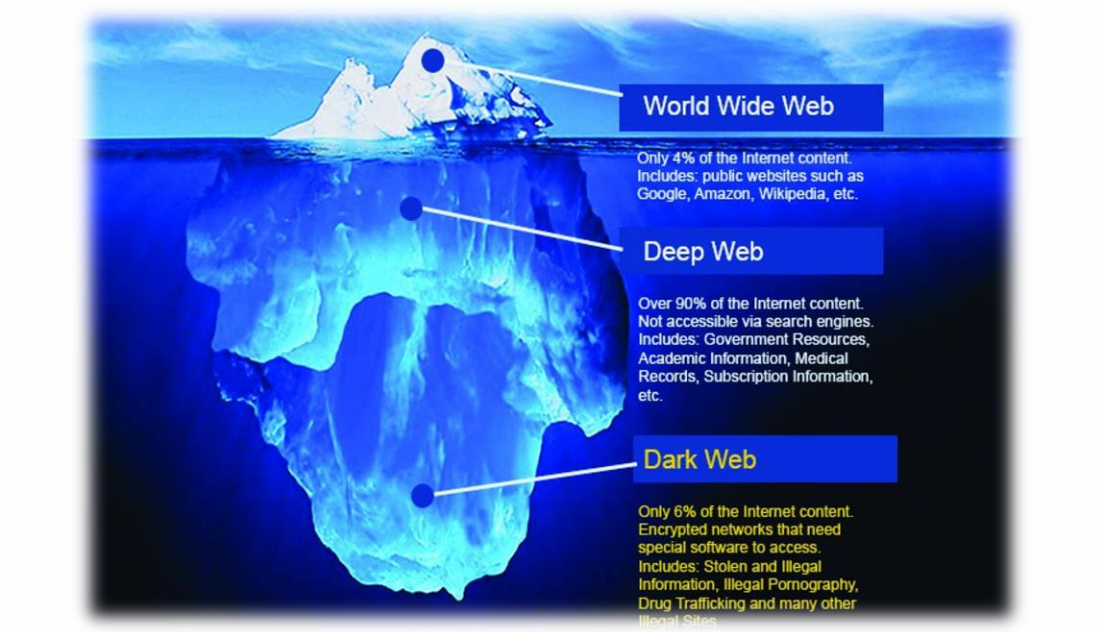
Now what? Well, now it's time to fire up Tails and do a little bit of tinkering.

How To Boot From Usb And Configure Tails

Bogged about your first boot? No worries. It always hurts the first time. Just follow these steps.

1. Keep the thumb drive in the USB.
2. Restart your computer.
3. After the splash screen appears, press the appropriate Boot Menu key.
4. Use your keyboard to select the corresponding drive letter. When you're done, hit Enter.
5. Wait for Tails OS to boot. Since this is the first time, it may take a while. Just be patient.
6. Configure Tails and deploy Tor + VPN. Yes, the latest version of The Onion Router has an in-built VPN.
7. Get ready to discover the dark and sometimes creepy wonders of the dark web.

How Do You Get On The Dark Web?



All done installing and configuring Tor? Great! Fire it up and let's surf. At first glance, Tor doesn't look that different from your regular browser – it has a search bar, lots of quick-launch icons, the peeled onion icon smack in the middle of the screen. So, now what? Well, let's start small.

Although content on the dark web is not as 'indexed' compared to the one on the clear web, you can still use search engines to find stuff. The Hidden Wiki and Grams are the heavyweights here.

Yay, now I found everything my heart longs for. Not quite: since the dark web relies on privacy and anonymity, search engines like the Wiki and Grams frequently return false results. No matter – good or not, the Hidden Wiki is a great place to start exploring.

The Hidden Wiki & Co.

Think of the Hidden Wiki as Wikipedia's evil twin – looks more or less the same, but contains links to various dark web categories: editor's picks, volunteer, introduction points, financial services, commercial services,

email\messaging, drugs (yes, it's the real deal), blogs & essays, hosting providers, hacking services, darknet radio (nothing shady about that; just some weird electronic tunes and, occasionally, a bit of jazz), literature (mostly resources on hacking, both ethical and black hat).

You can also find quick links here to the stuff that makes the dark web pitch-black dark: contract killers, rape, torture, or murder on demand, child pornography.

Fortunately, in Hidden Wiki, every website is followed by a brief description so that the user knows what to expect (or not). My advice to you would be to stick with the editor's pick. You can also take a look at the blogs & essays section if you want to find some nifty coding resources.

If you're feeling chatty, you can always access a chat room. Services like Random Chat connects you with random people using the same service. What happens after that, it's all to you.

You should stay away from everything labeled "porn", "card skimming services", "PayPal hacks", "firearms", "real fake IDs and passports".

Most are being kept under surveillance, not to mention the fact that you'll get exposed to some stuff that will definitely make you take several cold showers.

Hidden Wiki's not the only search engine online. Here are a couple of alternatives in case you get bored with Wiki.

- **DuckDuckGo** – also available on the clear web. The best thing about DuckDuckGo is that it doesn't track your searches. One can say that it's the Google of the dark web.

- **Torch** – considered the first dark web search engine, Torch boasts a database of several million onions links. Works just like Yelp. It even comes with recommendations, although most of them append websites like the

infamous **Silk Road**.

- **WWW Virtual Library** – if Torch and Hidden Wiki are old, the triple-W Virtual Library is Cthulhu-old; as in the elder god of search engines. What's even better is the fact the WWW Virtual Library contains info dating back to the beginning of the Internet: logs, documents, pictures, and everything in between.

  Fun fact: The Virtual Library was founded and, for a very long time, curated by none other than Tim Berners-Lee, the George Washington of the Internet. So, if you're looking for obscure Internet facts, very old documents, Berners-Lee's brainchild is the way to go.

- **Uncensored Hidden Wiki** – think regular Hidden Wiki is bad? Wait till you see the uncensored version. As the name suggests, it emphasizes very illegal activities like human trafficking, drugs, pornography went wrong, and other things that fester in the dark corners of the human mind.

- **ParaZite** – do you know the "want to get Lucky?" button in Google's search engine? The one that takes you on a random clear web site? Well, ParaZite does the same thing. Sure, you can use it like any run-of-the-mill search engine, but if you're feeling curious, you can also try the "feeling (un)lucky" feature. Proceed with caution and prepare to eject and torch the thumb drive.

Commercial Services

Believe it or not, the dark web even has online shops. And no, they don't all sell drugs or firearms. Some of them are, reportedly, legit and have great bargains. For instance, if you want to buy a laptop or a smartphone, you can try your luck in one of these shops. Of course, all transactions are anonymous and Bitcoin-driven. Sure, you can use other cryptocurrencies if Bitcoin's not your cup of tea.

The major issue with these websites is that a whopping 50 percent are fake, and there's no way of telling for sure if they'll deliver or not. By the way, most have shipping services.

Of course, you can't use your home address for dark web drop-offs, but apparently, they can ship all over the world, minus some Middle Eastern countries and North Korea. To tell you the truth, I was tempted into purchasing a Samsung Galaxy S10 Plus; it was only 250 bucks. My advice: look, but don't touch (buy).

Commercial Services You Should Visit When Browing the Dark Web

- **CStore** – any kind of electronics. You can make purchases in cryptocurrency or gift cards. They even accept full escrow.
- **Apple Palace** – everything Apple: laptops, desktops, phones, and accessories. All at ludicrously low prices.
- **EuroGuns** – the name says it all: guns sold on the European market. The website even boasts that it's the number one European arms dealer.
- **Kamagra for Bitcoins** – if your boomstick ain't working no more, you can try Kamagra, which is the dark web and cheap version of Viagra.
- **Gold & Diamonds** – site offers 'real' diamonds and gold. (Un)fortunately, it only ships to Germany and the United States.
- **PirateSec** – legit hackers, at your service!
- **Fake Passports** – I think it's self-explanatory.
- **SOL's United States Citizenship** – sells American citizenships; go figure.
- **Digital Gangster** – the most gangsta way to hack someone's computer. Apparently, these are Ronin hackers who can be hired for exploits, web hacking, password retrieval, and all-purpose espionage.
- **Onion Identity Services** – summer discounts for IDs and passports. Bitcoins only.

Email Clients

Always remember that the dark web is a people-centric community. So, it's only natural to find ways to keep in touch with your darknet buddies and\or customers. There are several email and IM services which you can use, and it's highly recommended to pick one if you want to step up your dark web game.

In terms of functionality, I don't think there are too many differences between regular IMAP, POP3, and SMT services and the stuff you can use to communicate on the dark web. Let's start with the email clients.

- **secMail** – full-fledged email service. Pretty simplistic in design: you can compose, send, and receive emails. All the great things about an email client, minus the tracking, eavesdropping, and other privacy issues.

- **Lelantos-** pay-to-use email service. Great security and privacy features, but it has one of the most unreliable and sidetrackable registration forms. Proceed at your own risk.

- **Bitmail.la** – another pay-to-use email client. Has many features like IMAP, SMTP, and POP3 support, and a 500MB mailbox. Apparently, a lifetime membership costs $0.60.

- **Mail2Tor-** a free email service which, reportedly, works on both dark and clear web.

- **Guerilla Mail** – creates a disposable email address.

- **AnonInbox** – pay-to-use email client. Supports IMAP, SMTP, and POP3; charges around 0.1 BTC per year.

- **Protonmail** – has both paid and free subscriptions. Boasts the browser-encrypted email technology.

Chat\Social Media

Right. Let's now talk about social media and instant messaging. Believe it or not, Zuckerberg's Facebook has a darknet version. It's mostly used for covert communication, anonymous tips submission, and stuff like that.

Sure, it's not as secure as the clear web version, but it's there and totally legal to use. Hidden Facebook is hardly the only social media client on the dark web. Check out the list below for the 'hottest' dark web clients.

- **BlackBook** – works pretty much the same way as Facebook: you can chat, send pictures and friend requests, post status updates, and join groups. Though competing head-to-head with Facebook Onion, BlackBook's prone to hacking. Reportedly, the client was disabled at least a couple of times in 2018.

- **Torbook** – very similar to BlackBook. Some claim that both of them rose at around the same time, despite the creators not knowing each other.

- **The Campfire** – gather around the campfire, folks to hear the tale of tales. The name's rather suggestive – a big chatroom; everybody can join, and the topics can be anything from the latest trends in the music industry to how you can hide a human body.

- **Lucky Eddie's Home** – scripted chat room that sports one of the most efficient file-uploading system on the dark web. Just like any IM app, you can send or receive messages, join or create groups, and send files.

- **MadIRC Chat Server** – if you're over 30, you certainly remember the mIRC era. Surprisingly enough, IRC off-spins are still being used today,

mostly for covert conversations or intranet communication. MadIRC Chat works just like a regular IRC – no or subscription required. Just pick a username and join in on the fun. It is advised that you not share any personal details because you may never know who's on the other side of the line.

- **Chat with strangers** – think Omegle, but on the dark web. Just fire up the client, connect to a chat room, and that's it. You can't send or receive files. Still, if you're lucky, perhaps you can partake in a scintillating conversation.

Journalism And Advocacy Groups

The dark web isn't just a place of eternal torment, teeming with drug dealers, human traffickers, and a hitman. It's also used by journalists, advocacy group members, and political refugees in hiding. Reuters, Fox, NBC, CNN – all of them keep open dark web channels to receive anonymous tips from whistleblowers.

Advocacy groups are also reaping the advantages of the darknet because, here, the term of censorship is as popular as HTTPS. And finally, we have political outcasts, refugees, and people who want to get in touch with the outside world, being from a totalitarian country that suppresses all means of communication and information.

Of course, there are your run-of-the-mill congregations, which will worship anything from Lucifer to the flying spaghetti monster.

If you're interested in subversive journalist, here are a couple of sites you can try visiting:

- **Soylent News** – a trans spectrum darknet news aggregator. Features webmaster-moderated forums on which you can submit comments. You can also get involved by either submitting tips or writing news.

- **ProPublica** – historically, ProPublica's the first major news outlet to feature well, a darknet outlet. With an activity spanning almost four years, ProPublica managed to expose power abuses and blow the lid on covert activities conducted by governmental institutions.

  Although quite young compared to other darknet news outlets, ProPublica's work was rewarded with five Pulitzer Prizes for Feature Writing, the last one being awarded to **Hannah Dreier**, the investigative journalist who covered the gangs of Los Angeles.

More On How To Stay Safe On The Dark Web

We already went through VPNs, anonymizing web browsers, and disposable operating systems, so I won't bother reminding you about those. Here some other things you can try to bolster your security.

1. Minimize or rescale your Tor browsing window

Sounds rather off, doesn't it? Well, there's a reason why it's recommended to browse with a minimized or rescaled window – you can be tracked based on your active window's dimensions (yeah, they really can do that). So, do yourself a favor and rescale that Tor window as much as you can before proceeding.

2. Tweak the security settings

Tor has an in-build slider which lets you adjust the level of security. Just click on the onion icon and choose Security Settings. Adjust the slider until the cursor points to the safest. This means that the JavaScript will be disabled by default on every website and some symbols and images will not be displayed.

3. Never use your credit and debit card for purchases

I'll go farther than that and say stay away from darknet shops. Maybe some of them are legit, but are you really willing to take that chance? Still, if you're really itching to purchase a new phone or God knows whatever, I would advise you to stick with Bitcoins or your favorite crypto coin. Using credit or debit cards for this sort of thing is like painting a big bullseye on your bank account while yelling: "come here and take my money."

4. Close Tails after finishing your session

When you're done surfing or shopping on the dark web, don't forget to shut down Tails. The major advantage of using a live OS such as Tails is that, on shut down, the OS wipes itself from the thumb drive you've installed it. That's why it's never a good idea to burn Tails on DVD.

5. Don't stick your nose where it doesn't belong

Great life advice, but it's even more valuable where the darknet is concerned. Keep in mind that many criminal organizations are using the dark web to communicate or sell merchandise.

Some of these channels are under watch. You may very well end up in the middle of a stakeout that could turn ugly. So, if the website looks fishy, close the tab, and forget about it.

How to Do a Dark Web Search? – A Basic User Guide

The Dark Web is a subset of the Deep Web, that part of the internet that doesn't get indexed by search engines like Google. When we talk about the Dark Web, that mainly refers to sites that are accessed through Tor Hidden Services. So can you do a Dark Web search?

Tor is an encrypted network that uses volunteer computing nodes to randomly move data packets from source to destination. Which makes it impossible to know who anyone on the other side of the connection is. So while you may be able to access a Dark Web site, you can't know where they are hosted. Also, they can't know who or where you are unless you divulge that information.

That's all wonderful, but if these sites are so hidden, how do you actually find them? If you can't just type terms into Google, how do people know where to go? To visit a Tor site you need its "onion" address, which is like a normal web URL but specialized for this anonymous service. The various ways you can find these addresses will be elaborated below and soon you'll be a pro at finding the sites you're looking for.

A Word on Using VPNs with Tor

Before we go over the actual sources you can use to find onion addresses, we need to talk for a minute about using a VPN when accessing onion sites through Tor. Although Tor is designed in such a way that no one can see which sites you are accessing or what information you're sending, there's still plenty of information leaking from your online activities.

Specifically, your service provider can see that you are using the Tor protocol, which might be considered suspicious by itself. Furthermore, they can log at what times you access Tor and how much data is transferred. That might seem harmless, but if the onion site ever gets seized or hacked, logs on their end could be correlated with those ISP logs, so it's not a non-issue.

If you use a VPN your ISP has no idea what you are accessing Tor at all. Of course, in some parts of the world using a VPN is also a suspicious act, but in most places, it's seen as a normal safety and privacy measure.

The Two Main Approaches to Finding Onion Sites

In your search for Dark Web sites, there are really only two places that you can look at. The first is the surface web. That is, the same web we all use every day for general internet applications. There are plenty of places you can go on the web that will list onion addresses.

The second approach is to visit certain strategic resources on the Dark Web itself. Which will then point you to the sites you were looking for.

Surface Web Resources

Why is it that sites can advertise onion links to Dark Web sites in plain sight in the surface web? Plenty of people are surprised by this, but if you understand more or less how it all works, it makes perfect sense.

First of all, Tor isn't illegal by itself. Although many authorities would like to create that impression, for the most part, there is nothing fundamentally wrong with simply browsing the Dark Web. Which in turn means there's also nothing wrong with listing onion domains.

Now, if you visit those domains and take part in something that is in fact illegal, that's a different story, but the bottom line is that there are plenty of places to find Dark Web site addresses online.

Reddit Repositories

Reddit is known as the "front page of the internet" and you can find Reddit boards on just about every possible topic you can think of. The Dark Web is no different and there's a whole community of people dedicated to discussing the Dark Web. This includes keeping tabs on any new onion domains and reporting when a site goes down or something else notable happens.

The Hidden Wiki on the Clearnet

The Hidden Wiki is probably the most famous repository of onion domains out there. It also claims to be the biggest, although that's hard to confirm. While the true face of this site is on the Dark Web itself, there's a version on the regular old world wide web.

Here you will find a massive number of categorized onion links, which include other sites that will lead you to even more results.

Dark Web Resources

If you want to find onion sites by using the Dark Web itself, there are some similarities and some differences compared to looking for them on the surface web.

Onion Repositories

Onion repositories include sites like the onion version of the Hidden Wiki. Which is again a good place to start to find other repositories. Unlike the surface web versions of the Hidden Wiki, the address tends to change. So you may have to look around surface web sites to find the latest working repository links.

Dark Web Search Engines

The term “search engine” might not be the best way to describe how these sites work. But from a user perspective, they look and feel sort of the same.

While you’ll find plenty of sites labeled as search engines on the Hidden Wiki, one worth bookmarking is Torch.

Are You Having Trouble Finding What You’re Seeking?

There is no single, straightforward way to find sites on the Dark Web. In fact, it’s only the sites that want to be found that you’ll dig up using the above methods. There’s an unknown multitude of onion domains out there. That

only a select few people know about and they'll never share it. Only sites that want visitors need to advertise after all.

What is the Dark Web, What's on it & How to Access it

This is how the Dark Web differs from the Deep Web, and how you can visit websites on the Dark Web using the Tor browser. We also explain why you probably shouldn't do that.

There's more: the Dark Web and the Deep Web loom in much shadier corners. You won't see any of this stuff in the results when you do a Google search, so wat exactly can be found on these dangerous sounding places? Should you even want to visit the Dark Web or the Deep Web?

Here's what you need to know.

What is the Dark Web?

The Dark Web refers specifically to websites that exist behind multiple layers of encryption and cannot be found by using traditional search engines or visited by using traditional web browsers.

Almost all sites on the so-called Dark Web hide their identity using the Tor encryption tool. You may know Tor for its ability to hide your identity and activity. You can use Tor to spoof your location so it appears you're in a different country to where you're really located, just like when you use a VPN service.

When A Website Is Run Through Tor It Has Much The Same Effect.

Indeed, it multiplies the effect. To visit a site on the Dark Web that is using Tor encryption, you have to use Tor. Just as your IP address is bounced through several layers of encryption to appear to be at another IP address on the Tor network, so is that of the website.

Put simply, there's a lot more secrecy than the already secret act of using Tor to visit a website on the open internet - for both parties.

Thus, sites on the Dark Web can be visited by anyone, but it is very difficult to work out who is behind the sites. And it can be dangerous if you slip up and your identity is discovered.

You can also read our in-depth guide to using Tor if you want to know more about using the web anonymously and sending messages securely.

MORE . . .About the Stuff You'll Find on the Dark Web

Not all Dark Web sites use Tor. Some use similar services such as I2P, for example the Silk Road Reloaded. But the principle remains the same. The visitor has to use the same encryption tool as the site and - crucially - know where to find the site, in order to type in the URL and visit.

Infamous examples of Dark Web sites include the Silk Road and its offspring, such as Dream Market. The Silk Road was a website for the buying and selling of recreational drugs, and a lot more scary things besides. But there are also legitimate uses for the Dark Web.

People operating within closed, totalitarian societies can use the Dark Web to communicate with the outside world. And given recent revelations about US- and UK government snooping on web use, you may feel it is sensible to take your communication on to the Dark Web.

The Dark Web hit the headlines in August 2015 (and many times since) after it was reported that 10GB of data stolen from Ashley Madison, a site designed to enable bored spouses to cheat on their partners, was dumped on to the Dark Web.

Hackers stole the data and threatened to upload it to the web if the site did not close down, and they eventually acted on that threat. The spouses of Ashley Madison users received blackmail letters demanding they pay $2500

in Bitcoin or have the infidelity exposed.

In March 2015 the UK government launched a dedicated cybercrime unit to tackle the Dark Web, with a particular focus on cracking down on serious crime rings and child pornography. The National Crime Agency (NCA) and UK intelligence outfit GCHQ are together creating the Joint Operations Cell (JOC).

There is a DIFFERECE between the Dark Web vs Deep Web

Let's me this perfectly clear. Although all of these terms tend to be used interchangeably, they don't refer to exactly the same thing. An element of nuance is required. **The Deep Web refers to all web pages that search engines cannot find.**

Thus the 'Deep Web' includes the 'Dark Web', but also includes all user databases, webmail pages, registration-required web forums, and pages behind paywalls. There are huge numbers of such pages, and most exist for mundane reasons.

You Can Search the Deep Web Easier than You Think

If you can't find it with Google, then it doesn't exist at all? As great as Google is in locating info online, the truth is that with it, you can find only a small portion of the info that exists the world.

Google indexes billions of pages, but there are hundreds, if not thousands, of other pages that for one reason or another are not present in its index. These pages are hidden in the debris of the Deep Web, and chances are you will be able to find them if you know how to search.

The Deep or the Dark Web? Which one is you?

When people speak about pages not indexed by Google, maybe your first idea is about the Dark Web. While the Dark Web, also called Darknet, fits the

description of sites/pages not indexed by Google, the Dark Web and the Deep Web are not the same thing.

An example of a Deep Web page is a closed group on Facebook. Since the page is accessible after a login only, and Googlebot can't log in to access it, the page is not indexed. However, when you log in to this group, you can see the page. Similarly, if the page requires payment to gain access, Googlebot can't index it, but you can view it after you pay.

No-follow or broken links, or dynamic pages generated on the go after a search query from a user, also stop search engines from indexing pages, but you as a human can access this information. Info in the form of an image/video or other formats search engines don't understand but humans do is another example of Deep Web content. These pages are accessible with a simple browser, and generally they use the http (or https) protocols.

On the other hand, the Dark Web uses a different routing protocol with built-in encryption. Two popular protocols are TOR and I2P. The Dark Web contains lots of illegal resources, too, and search engines by no means will index these, even if they could.

Now, after I explained the difference between the Deep and the Dark Web, let's see what you can do to find stuff in the Deep Web.

1. Try Other Search Engines

Sometimes a page is not accessible by Google (for one reason or another) but is indexed by other search engines. Technically speaking, in this case the page isn't in the Deep Web (because it's accessible via a search engine), but for anybody whose search starts and ends with Google, the page is not there. If you get in the habit of occasionally using other search engines, such as DuckDuckGo, a local search engine, or even Bing, in addition to Google, you might be surprised by the amount of good stuff you can find with them.

2. Find the Main Page with Google and Go on Your Own

In other cases Google has the main page of a site only. This happens with sites that require login or payment or that have no-follow links Google didn't index. If this is the case, it's easy – find the main page with Google, and then explore the site on your own. If the site has a search functionality, your task is even simpler.

3. Try Google Books or Go to a Library

If you know a document exists, but you can't find it with Google Books, you can go to a library, especially an academic one. Many libraries at colleges and universities subscribe to paid databases, and chances are you will be able to use these, maybe even for free.

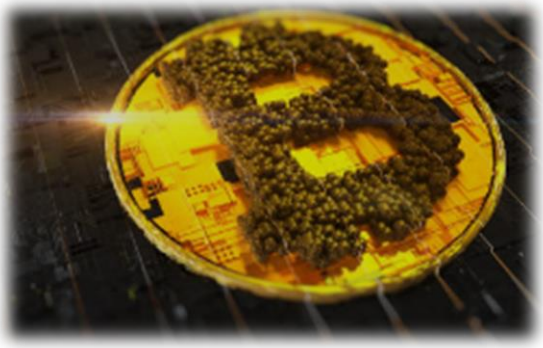
4. Try the Deep Web Search Engines

As surprising as it sounds, the Deep Web has search engines of its own. In many aspects, such as user interface or functionality, these search engines are light years behind Google, but don't judge a book by its cover.

There are really a lot of these engines, and it might take quite a lot of time to find what you want. Even worse, sometimes you might spend days or weeks to no avail. Check this huge list of Deep Web search engines and locate the ones in your area of interest. If you are looking for older versions of current pages and stuff that used to be online but isn't anymore, try the The Internet Archive project.

It might be a bit harder to find stuff in the Deep Web, but if you are looking for highly specialized stuff, you might have more luck there than with general search engines.

Interesting and Informative Websites on the Dark Web



The dark web is that mysterious part of the web that most people only get to with the Tor browser. Websites with the suffix '.onion' host hidden services that aren't accessible through regular browsers (unless you do a lot of tweaking).

The Tor-browser, however, enables you to visit these services while also giving you a layer of anonymity. When the dark web is in the news, it is often associated with illegal practices. There are countless stories of "dark markets" where you can buy anything illegal such as drugs, weapons or fake passports.

There is an element of truth to this, but quite often, these stories are overhyped, untrue, and exaggerated. Usually, the more positive and sometimes surprisingly wholesome things you can find on the dark web are never mentioned.

Don't know how to get on the dark web?!

A list of websites is right here if you wish to visit the dark web, but want to visit it in a secure manner. Some websites on the list are quite serious, while others are just very silly. Happy exploring!

Caution: Safety first when accessing the dark web

If you venture further on the dark web, it is wise to take some safety measures. Since the dark web is unregulated, there is an increased risk

of malware infections and/or cyber criminals going after your data. Make sure you have antivirus software installed and that you use a VPN.

A VPN encrypts and secures all your internet traffic, safeguarding your privacy online and protecting you against certain forms of cyber crime. To get started, try out NordVPN. For less than $5 per month, NordVPN protects all your internet data with heavy encryption.

Plus, you become anonymous when using NordVPN, since your IP address will be hidden. This prevents others from tracing your online steps. NordVPN offers a 30 days money-back-guarantee, so you can try it without risks.

NordVPN9.1

- Excellent protection and a large network of servers
- Nice and pleasing application
- No logs

If you want to know more about this part of the internet and how to get there you can visit our page about the dark web.

Section 1: Search

Although the dark web does not host any search engines like Google, it is still possible to navigate the landscape of the dark web through search engines and directories, if you know where to look. A number of the following sites might help you along your way.

Hidden Wiki

The Hidden Wiki is a dark web Wikipedia where you can find links to different websites on the dark web. As you may notice in this article, the URLs of dark web pages are often nonsensical. This makes it difficult to find the website you're looking for.

On the Hidden Wiki they do a lot of the searching for you. Moreover, they provide informative pages on a range of topics that can be an interesting read.

Watch out that you do not click on a link to something you do not want to see, because the Hidden Wiki doesn't just index legal websites. In fact, there are many different "Hidden Wiki" sites out there. The Hidden Wiki used to be known for hosting, or at least, indexing a bunch of pedophile websites and has therefore been the subject of cyberattacks by the FBI and Anonymous.

Many copycats and spin-offs of the Hidden Wiki have also been created. Don't be surprised if you come across "The Official Hidden Wiki" or "The Uncensored Hidden Wiki". It is best to stay away from these spin-off sites, however.

Most Hidden Wiki sites to this day provide links to some parts of the dark web you would not want to visit. The best way to deal with this is to just stick to the categories that are relatively risk-free.

Link to the Hidden Wiki:
http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

DuckDuckGo

DuckDuckGo is a search engine that is also available on the surface web. As opposed to other search engines, DuckDuckGo does not collect or share any of your personal information. The search engine is ideal if you want to be completely anonymous on the web.

On the dark web it is used because it also shows .onion websites. Most regular surface search engines do not index .onion websites. Thus, a regular search engine won't bring you anywhere on the dark web, but DuckDuckGo will.

Link to DuckDuckGo: https://3g2upl4pq6kufc4m.onion/

Candle

This aptly-named site is there to help you see your way through the dark web, figuratively speaking. Candle is a search engine for just the dark web and functions basically just like Google, except that it is nowhere near as useful. The Dark web simply isn't designed to be neatly organized and indexed.

The whole purpose of the majority of services on the dark web is to remain hidden, except for a select group of people who are "in the know". This is why Candle should be seen as a minor tool, a small candle in a long dark hallway.

The search engine will allow you to see just a tiny bit clearer in the dark, but not much. Also be wary of clicking any links that the Candle search-engine offers up, as they are not filtered for malicious or illegal content. As always when browsing the dark web, exercise common sense and remain vigilant.

Link to Candle: http://gjobqjj7wyczbqie.onion/

Not Evil

This is another search engine on the dark web. This site is interesting as it appears to directly contradict its own mission statement, which is to be a "contribution to what one hopes is a growing shield against the tyranny of an intolerant majority." They do not accept donations and they strictly forbid illegal content such as child pornography, weapons, narcotics or any other illegal content.

This does not prevent the site to host links to illegal hidden services, though. If you look up "cocaine", for example, the Not Evil search engine will find some links to online markets, guides, or referral sites associated with the illegal substance. Not Evil also hosts a chat service where any member can create a new topic. The these topics range from disturbed to the depraved. Most of the content is, however, spam.

It is reasonable to assume that hackers, scammers, and even law enforcement officials can be found on such chat services. Law Enforcement officials sometimes venture onto the dark web in an attempt to catch wrongdoers and might even attempt to trick you into illegal activities as part of a "honey-pot operation".

Link to Not Evil: http://hss3uro2hsxfogfq.onion/

SearX

Searx is yet another search engine you can use on both the regular and dark web. The advantage of SearX is that you can make your search queries incredibly detailed. You can look for files, images, maps, music, news, science, social media posts, videos, and much more. So, if you are looking for something incredibly detailed, SearX is the search engine to use.

Link to SearX: http://ulrn6sryqaifefld.onion/

Section 2: Dwell

The dark web is full of surprising sites. One of them is Facebook. Although it is not recommended for you to log into Facebook for any kind of online protection, it is striking this social media site has such enormous presence on the dark web.

Facebook

This is a mirror website of the real Facebook. By creating a Facebook account through the dark web you can attempt to do so completely anonymous. However, this takes a lot of work, because, as we know, Facebook likes collecting all the data they can.

More importantly, this mirror version of the social network is a way around government censorship. Some regimes censor social media or make them completely inaccessible for their people. They do this to eliminate any form of opposition. By using the dark web version of Facebook people can attempt to stay anonymous.

Link to the Facebook mirror: https://www.facebookcorewwwi.onion/

BlockChain

Although Bitcoins are only just now becoming popular with the general public, it has been the currency of the dark web for years. It will come as no suprise that there are many cryptocurrency websites on the dark web. On the BlockChain website you can manage your cryptocurrencies as well as, buy and sell them.

Moreover, you can check how your stocks are doing to see if it is the right time to buy or sell. Since bitcoins are used to buy products on the darkweb, it is no wonder there also is a virtual wallet.

Link to BlockChain: https://blockchainbdgpzk.onion/

Bibliomaniac

Among other things, the dark web is a place where ideas about a large range of issues are shared. Moreover, intellectual conversations are encouraged. There are many websites on the dark web that offer books or online book clubs and Bibliomaniac is one of them. Take a look at the great wealth of knowledge if you find yourself on the dark web someday.

You can truly find any book on this website. Watch out that you do not download any copyrighted material, because that is illegal.

Tor Metric

On the Tor Metric you can find more information about the Tor Project. If you are interested in privacy and how the Tor project works, this website can give you some insight. Moreover, if you're researching Tor and the dark web for a school project this website can help you with statistics.

Among other things, you can see how many people use the Tor browser and how many .onion websites there are. The statistics of Tor users can also give you a good indication of how much activity there is on the dark web, how many hidden services exist, and where most users on the dark web are from.

Some fun facts:

- Only about 6% of Tor users use the browser to access the dark web
- Some of the most prolific Tor users are from countries with relatively small populations, such as Germany or the Netherlands.
- The Tor browser has been downloaded around half a million times in 2019 alone

Link to Tor Metric: http://rougmnvswfsmd4dq.onion/

Hidden Answers

Hidden Answers can be described as a dark web version of Reddit or Quora. You can ask any question you like, without any censorship. Others in the community will try to answer your queries. It can also be fun just to look around. Do remember, that this an unfiltered part of the internet and you might encounter conversations that you do not want to see.

This is also a great place to ask questions about the dark web, if you are new to this part of the internet. It's a safer to option to visit some dark web subreddits for specific questions on the dark web, however.

Link to Hidden Answers: http://answerstedhctbek.onion/

11. Secure Drop

Secure Drop is a place where whistleblowers and journalists can meet. The dark web is the only way that whistleblowers have a chance to share their information without being certain that they will be tracked. Whistleblowers have damaging information about a company or government and try to share this with journalists.

If they do so on the surface web, they will likely be traced and, in some cases, punished. Secure Drop is an .onion website that protects the privacy of whistleblowers and journalists the world over.

Many **important publications** have realized the power of anonymous whistleblowers on the dark web and set up their own SecureDrop URL. Some notable examples include:

- Forbes: http://t5pv5o4t6jyjilp6.onion/, The Financial Times:
- http://xdm7flvwt3uvsrrd.onion/ and
- Reuters: http://smb7p276iht3i2fj.onion/.

Link to Secure Drop: http://secrdrop5wyphb5x.onion/

Section 3: E-mail

There are plenty of email providers out there besides Outlook and Gmail. Have a look around at some of the amazing services that are provided for free.

12. Protonmail

Protonmail is an encrypted email service that prides itself among the very best of the e-mail clients out there.

Link to Protonmail: https://protonirockerxow.onion/

13. Secmail

Secmail has proved to become one of the most used dark web email providers of the past few years. Although they only provide a measly 25 mb per user, this tends to be more than enough for PGP-encrypted messages.

Link to Secmail: http://secmailw453j7piv.onion/

14. MailPile

“Mailpile is an e-mail client!
Mailpile is a search engine and a personal webmail server.
Mailpile is an easy way to encrypt your e-mail.
Mailpile is software you run yourself, on your own computer.”

Link to: http://clgs64523yi2bkhz.onion/

Section 4: Miscellaneous

15. The Chess

On this website you can play a game of harmless chess with a stranger, nothing more, nothing less, just chess. They present you with the extensive rules of the game and by making a simple account you can start playing. The website aims to create a calm place where chess lovers can meet.

Link to The Chess: http://theches3nacocgsc.onion/

16. Tor Kittenz

The dark web has an interesting relationship with cats. A famous dark web cat website is Anonymous Cat Fact, however is seems like it no longer exists. Luckily, the dark web is full of random websites with cats. On Tor Kittenz you can see random pictures of cats. You can find a lot of these silly types of websites on the dark web.

Link to Tor Kittenz: https://mqqrfjmfu2i73bjq.onion.link/

Warning

Curiosity is a beautiful thing, but remember it also killed the cat! It can be interesting to take a look on the dark web, but it is also quite dangerous. Before you know it you could have clicked on a corrupted link and your computer might be infected with malware. For this reason, we advise you not to go there if you do not have a good reason to do so.

If you do want to have a look around, make sure you have some security measures in place to protect yourself against any online attacks.

Security Measures

Visiting the dark web is not without risks, which is why we recommend you to take the following measures to protect you and your device.

First of all, you need good anti-malware software. To prevent your device from becoming infected with viruses or spyware you need to install good anti-malware. This type of software is essential, even when you're only browsing the surface web.

Secondly, you need to find a good VPN. A VPN (Virtual Private Network) is software that encrypts all of your internet traffic and hides your real IP address. Just to be safe, it's best to use a VPN so nobody will be able to see

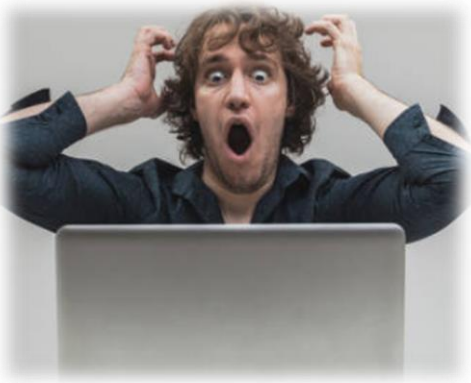
that you're visiting the dark web. Moreover, hackers on the dark web won't be able to trace your actions back to your personal IP address. Some good VPN providers are, ExpressVPN, NordVPN, and IPVanish.

Finally, you should use your common sense. Do not click on any links you do not trust and do not fill in any personal information on the dark web.

Conclusion on this subject

The dark web sounds mysterious and maybe even scary, but some of the .onion websites are very mundane. For regular internet users there isn't really a good reason to go there. But if you do, you might want to visit one of these 10 websites. Remember that there is a lot of seedy business going down on the dark web, so do not click on anything you do not trust.

Why do Most People FEAR the Dark Web? Don't Buy the Hype!



Key Findings

The collection of onion sites that is sometimes called the dark web is often portrayed as a vast and mysterious part of the internet. In reality, the number of onion sites is tiny compared to the size of the surface web. A count of live reachable onion site domains comes to less than 0.005% of the number of surface-web site domains.

Out of about 55,000 onion domains found, only around 8,400 onion domains had a live site (15%). The popular iceberg metaphor that describes the relationship of the surface web and dark web is upside down.

These onion sites are disorganized and unreliable. Scams are prevalent, such as a typosquatting scam that claims to have successfully defrauded users of over 400 popular onion sites, netting thousands of dollars in Bitcoin from victims.

Uptime even on popular dark web sites is well below the 99.999% “five nines” availability that is expected for reputable companies on the surface web, and onion sites regularly disappear permanently with or without explanation.

From a language standpoint, onion sites are more homogeneous than the surface web. We observed that 86% of onion sites have English as their primary language, with the next two most common being Russian with 2.8% and German with 1.6%. On the surface web, researchers report English is at the top with only 54%.

The idea of a dark web that is hidden and mysterious is more likely an extrapolation of a tiny portion of these onion sites — a set of invitation-only and unpublicized communities buried in the most shadowy corners of this part of the internet. On the surface web, popular websites will attract inbound link counts in the millions or more.

About the onion site crawl, the site with the highest inbound link count was a popular market with 3,585 inbound links. An onion site offering help setting up onion servers had 279 inbound links.

In contrast, we looked at what we view as the top eight onion sites most respected in the criminal community and found that the most visible had a maximum of 15 inbound links with an average of only 8.7 inbound links per site. It is this tiny slice of the dark web that is truly dark.

A Responsible Way To Travel The Dark Web

Thanks to a certain online drugs marketplace called “Silk Road”, you may have become aware that there is another version of the Internet out there. One which cannot be accessed by any ordinary browser or indexed by any ordinary search engine.

It is called the Dark Web, not to be confused with the *Deep Web*, which are websites which cannot be ordinarily accessed due to paywalls or password-protected login pages (such as online banking).

The Dark Web has some legitimate valid uses, such as protecting the free speech of dissidents and activists in countries run by oppressive regimes (such as China). But mostly, the Dark Web has been referred to as the “dark underbelly of the web”. A lot of it comprises drugs, pornography, gambling, hitmen, and various other criminal enterprises.

That being the case, you might ask why it is worth even looking at it if you are not inclined that way. I would argue that it is worth taking a look, even if it’s just for curiosity’s sake. It’s a fascinating glimpse at another world.

The Onion (Tor) Browser

To access the Dark Web, you need a specialised browser. Using Firefox, Chrome or Safari is not going to work. To access the Dark Web, you need the Onion Browser (otherwise known as Tor). You can download and install the Tor Browser by going to the Tor website.

Being a modified Firefox browser, the Tor browser can access regular internet sites as well, but one of its main purposes is to access the dark web. Tor will protect your location by running your internet traffic through several “Tor Relays” (virtual private networks) so Tor runs much slower than a regular browser. Such is the price for your privacy.

The Dark Web’s URLs

The Dark Web runs on its own URL format, namely the **.onion** format. So whereas a regular link might be http://www.website.com, a Dark Web link would be http://thg67klkk4ksl9s.onion.

As you can see, a Dark Web link does not use .com or .net, .org, or any of the other usual website domain endings. And a Dark Web link also does not have a proper name like “Google” or “Yahoo” or “eBay”.

Instead it is a random selection of characters which makes Dark Web sites hard to find and guess. This is part of what makes the Dark Web attractive to criminals and others who want to operate under the radar.

Since Dark Web sites go up and down all the time, and figuring out the URL is pretty much impossible, even Dark Web *search engines* are notoriously unreliable! But if you are a blogger in say Beijing, you wouldn’t want your Dark Web site indexed anyway by a search engine for the government to track you. You would instead rely on word of mouth from trusted supporters to find you.

Diving Into The Dark Web

Once you have the Tor browser installed and open (which is extremely easy and requires no special configurations), it’s time to look at some sites.

I should say before continuing that although Tor is a modified Firefox browser, you should NOT install any Firefox extensions. There are two extensions already pre-installed – NoScript and HTTPS Everywhere. They are there for your security – do not install any others.

With that in mind, also remember that the Dark Web is the Wild West of the Internet. There are no rules and you are going to encounter some seriously creepy and dangerous individuals if you venture onto forums and chat rooms.

Therefore do not reveal any personally identifying information about yourself and be extremely cautious about what links you click on. If you click on child

pornography, for example, you will be putting yourself in serious legal jeopardy if the police is monitoring the site. **Ignorance is not a defence**.

Search Engines & Directories

Almost everyone universally agrees that the best place to start with the Dark Web is Ahmia.fi . This is a Dark Web search engine which can be accessed on the regular Internet too.

Making your way around the Dark Web involves just looking at search engines and directories and basically browsing until you find what you want. Each of you will have your own different interests so it would be pointless to send you in one particular direction.

So here are a list of some search directories and pages that will send you off scurrying down the Dark Web rabbithole. Let us know in the comments what you find. Some of these links may not be available when you try to visit, but they will come back later.

If the site is continuously down, use Ahmia to search for the site's new location.

Other Deep Web Terms

Dark web — the term alone sounds sinister. And it's true, plenty of illegal activity can take place in this part of the Internet. But accessing the dark web isn't illegal. And not every site found there is dealing in criminal activities.

The dark web is much like the world of Google, Yahoo, and all the other sites you visit each day. But sites making up the dark web are hidden from view. You can only access these sites with special browsers, The Onion Router, or TOR, being the best known of them.

There's a difference, too, between the dark web and the deep web. The deep web also holds hidden sites. But these sites are mostly benign. The deep web

is home to everything from password-protected email accounts, the private intranets run by businesses, government databases, and private sites that users can only access with a log-in name and password.

The dark web is a subsection of the deep web. Many of the sites on the dark web do focus on illegal activity. You can buy guns or drugs illegally on the dark web. You can visit online marketplaces that sell hacked passwords and bank accounts. Illicit pornography is available here, even child pornography.

But not everything in the dark web is illegal. Residents who live under government regimes that censor social media and punish dissent can rely on the dark web to reach out to others and publicize the wrongs committed by their governments.

Others can research medical information that they might otherwise be embarrassed to study. Journalists often use the dark web to communicate with sources whom they want to protect.

Understanding the dark web can be confusing if you've never visited this corner of the online world. The growth of the dark web has spawned a whole new language, one that might be unfamiliar to those who aren't tied into the underground economy of the dark web. But we can help.

Just check out this expansive glossary of terms to gain a better understanding of how the deep and dark webs function.

Alias

Many of the people searching the dark web prefer to remain anonymous. This isn't surprising considering that many visit to do something illegal, whether that means buying drugs or trying to acquire someone's Social Security number. It's why many visitors log in with an alias, a screen name designed to keep their real identities hidden.

Not everyone who uses an alias, though, is involved in criminal activity. Political dissidents, for instance, might rely on aliases, too.

Bitcoin

Bitcoin is basically the currency of the Dark Web. It's a virtual currency — the most popular one — that visitors to the dark web can use to purchase items from online marketplaces or to subscribe to sites. Bitcoin is popular on the dark web because people can buy it anonymously.

This gives them the chance to make illegal purchases without being tracked. People can also use Bitcoin to make legal but potentially embarrassing purchases, such as paying for pornography.

Cybercriminals often use Bitcoin in ransomware scams. These criminals will take over your computer, locking it up, until you pay a ransom, using Bitcoin to make your payment.

Blockchain

A blockchain is a type of database — made up of blocks of information — that records a series of transactions. The information in a blockchain is distributed across a series of users or computers, meaning that there is no one central person or agency that has control over the transactions recorded in it.

The Bitcoin blockchain is one of the most important, a public record of all Bitcoin transactions. As with all blockchains, past transactions, once added to the chain, can't be altered or erased.

Carding

There is a lucrative market on the dark web for credit card information. Hackers often offer working credit card numbers for sale at online marketplaces. Other criminals can purchase these numbers and then run up

thousands of dollars in fraudulent purchases while using them.

Carding is the term used to describe the practice of stealing credit card information and selling it on the dark web. How serious is this problem? The cybersecurity firm Sixgil in a report said that there were more than 23 million stolen credit and debit card numbers for sale on the dark web in the first half of 2019.

Clearnet

You know that the dark web is the mostly hidden part of the Internet. The Clearnet, though, is another term for the traditional Internet we all know. This is the Internet that is home to the sites you visit every day, from the home page of your online bank to your favorite news sites, Facebook, Twitter, and YouTube. Anything you can access with a traditional browser such as Chrome is part of the Clearnet.

Cryptocurrency

You can consider cryptocurrency to be a type of money, one that is used commonly across the dark web. Unlike dollars, pennies and quarters, though, cryptocurrency is virtual or digital.

It consists of nothing physical. Visitors to the dark web often use cryptocurrency — including Bitcoin, the most common form of cryptocurrency — to purchase items both **legal and illegal**.

Why? It's difficult to trace cryptocurrency, which makes it the perfect currency for customers who want anonymity. Cryptocurrency is also decentralized, meaning that it is not issued from a central point, but instead on a peer-to-peer basis.

Darknet

The darknet is another name for the dark web. The darknet is the home to hidden websites, sites that you won't find during a typical Chrome or Bing search. You'll need special browsers and tools to explore the sites that exist on the darknet.

Doxing

Doxing is often used as a form of revenge. It's when someone posts the personal information — or documents — of someone online. The goal when doxing is to expose the true identity of someone who has been operating in anonymity.

You might wonder where that name comes from. It's a shortened form of the phrase "dropping dox," meaning posting documents that could identify someone who prefers to remain anonymous.

Encryption

When data is encrypted, it is scrambled, making it unrecognizable. This is important: It's a key way to protect important information, both financial and personal, on the web. Often, you'll need an encryption key to open encrypted data.

But what if you are sending financial information to your bank or credit card provider? Today, most websites use something called Secure Sockets Layer, a way to encrypt data that is being sent to and from a site. This form of protection keeps cyberthieves from stealing that sensitive data while it is being transmitted. You'll know a site offers this protection if its address starts with "https://" instead of "http://."

Firewall

Businesses, financial institutions and government agencies rely on firewalls to protect their websites from cybercriminals. A firewall, as its name suggests, is a network security device that monitors traffic both incoming and outgoing and decides whether to allow or block that traffic. Firewalls make this decision based on a set of programmed security rules.

This protection isn't just for businesses, though. You can protect your own computer by installing a host-based firewall. A host-based firewall is stored on a single computer. These firewalls can serve as an early line of defense against cyber criminals and malware.

Honeypot

One way that security experts study cybercriminals and online attacks? They set up honeypots. A honeypot is a computer or computer system designed to mimic something that would attract the attention of cybercriminals. Like honey to bears, the honeypot is too sweet for criminals to ignore.

Credit card providers might set up a honeypot that looks like a database of credit card numbers. When hackers attack it, the bank's security experts can study where cybercriminals are coming from and how they are attacking. Security pros can then make changes to better protect their important data.

In 2015, security experts created a fake online railway control system as a way to study how hackers could attack systems when their goal was to put the public in danger. During a two-week period, the HoneyTrain was the victim of 2.7 million attacks.

IP address (aka Internet Protocol)

Every device connected to the Internet — including your laptop, smartphone, and tablet — has an IP address that identifies it. This IP, or Internet Protocol, address is a unique series of numbers separated by periods. Think of your IP

address as you would your home's street address: It identifies your device when you're online.

Your IP address, though, isn't always the same. If you work from home, you'll have a different IP address than if you're connecting at your local public library or nearby coffee shop. You'll also get a new IP address if you change your Internet Service Provider.

Malware

Malware is malicious software that can damage your computer. You can infect your computer with this software by downloading it accidentally from websites or opening an infected attachment in an email message. You might download a file online without realizing that it hides malware.

What does malware do? That depends. Some malware allows cybercriminals to take over your computer behind the scenes. Other malware will copy your key strokes and steal your passwords, allowing criminals to access your personal and financial information. Some malware might freeze your computer's most important systems and demand you send ransom money to a criminal.

Sandbox

Want to provide extra protection for your devices against viruses and malware? You should start with a good antivirus security software. But to boost your cyber safety, make sure your antivirus suite includes sandboxing applications.

Sandboxing forces the programs on your computer to run in an isolated environment, basically boxing them off from the rest of your machine. The benefit here is that programs running in the sandbox have only limited access to the other files and systems on your computer or other devices. When

applications are running in a sandbox, they can't make permanent changes to any of your systems.

You want to make sure, then, that your antivirus program sandboxes applications when you are using them. For instance, your antivirus program should automatically run your browser in the sandbox so that any malware on your computer won't copy your passwords or online financial information.

Spoofing

How do hackers get all those credit card and bank account numbers that they sell online? Spoofing is one method. Criminals send spoofed emails that look like they come from someone's bank or credit card providers asking them to, perhaps, click on a link to make sure that their accounts aren't shut down. When users click, they are taken to a fake web page that asks them to enter their account information. Once users do this, the hackers can steal this information.

The lesson here? Never click on a link in an email, even if it looks legitimate. And never send your financial information when your "bank" asks for it. Instead, call your bank or credit card company to ask if they really do need this information.

Tor (aka The Onion Router)

Tor, which stands for The Onion Router, is a browser that lets you search the Internet anonymously. It's also a browser that people commonly use to access and search the dark web. With this browser you can find sites with the .onion suffix, sites hidden from other popular browsers such as Chrome.

To download the browser, visit torproject.org. Even with the browser, though, finding sites on the dark web isn't easy. Remember, these sites are largely hidden. You might start by visiting the many lists of dark web sites

you can find on the Internet. Just be careful: Many of the sites on these lists specialize in illegal activity.

VPN

Using a VPN, or virtual private network, is an important step in protecting your privacy while online. VPNs, then, are popular among people surfing the dark web who'd prefer to remain anonymous to Internet Service Providers, hackers and government bodies.

A VPN is a private server that you sign up with, either for free or, for possibly more reliable privacy protection, for a charge. When you connect to the Internet, your computer will first log into this private outside server before it accesses the web.

This can help boost your online privacy. The only people who will see what sites you visit, files you download or links you click will be your VPN provider and the people behind the sites you visit.

Did You Know . . . The Dark Web As You Know It, Is A Total Myth?

After the conviction of Ross Ulbricht, the owner of the drug marketplace Silk Road, and a stream of articles claiming that the Islamic State is using secret websites to plan out attacks, this hidden part of the Internet is being talked about more than ever.

But for the most part, the story you've been sold about the dark web is a myth.

I know this because I've been there. Since 2013, I've interviewed the staff of drug marketplaces about their paid DEA double-agents, tracked how technologically sophisticated pedophiles cover up their tracks, and also discovered that active Uber accounts were being sold on the dark web for as little as a dollar each.

I've also learned that the real story is not at all the one you commonly hear—the tale of a gigantic space below our usual web, where hard-to-find vices are traded among sordid individuals totally beyond the grasp of the authorities. That is not what the dark web is.

The Rest of the Web Is Just as 'Dark'

You'll be told that it is home to several nefarious things: stolen data, terrorist sites, and child porn.

Now while those things may be among what's available on the dark web, all also are available on the normal web, and are easily accessible to anyone,

right now, without the need for any fancy encryption software.

For years there have been sites where you can instantly buy a stranger's Social Security Number, date of birth, full name, address and phone number for under a dollar, or others that host reams of stolen credit card details, ripe for a fraudulent spending spree.

Terrorist forums are also hiding in full view of anyone with an Internet connection. Regular websites allow extremist supporters and prominent jihadis alike to communicate with one another and post brutal propaganda videos.

Al Qaeda's first forum was launched way back in 2001, and although that site was shut down, a handful of other violent Islamic extremist sites continue to exist on the normal web and are used heavily today.

There are only shreds of evidence that the Islamic State is using the dark web. One apparent fund-raising site highlighted by the Washington Post had managed to garner exactly 0 bitcoins at the time of writing, and this was also the case with another I discovered recently.

It's worth pointing out that both of those sites simply claimed to be funneling the cash to the terrorist group, and could easily have been fakes.

And yes, child porn is accessible on the normal web. In fact, it is rampant when compared with what's available from hidden sites. Last year, the Internet Watch Foundation, a charity that collates child sexual abuse websites and works with law enforcement and hosting providers to have the content removed, found 31,266 URLs that contained child porn images. Of those URLs, only 51 of them, or 0.2 percent, were hosted on the dark web.

It's More Like a Dark Nook

What we call the dark web is tiny. The World Wide Web has swelled to over a billion different sites, while current estimations put the number of Tor

hidden sites at between 7000 and 30,000, depending on what methodology you follow.

That's 0.03 percent of the normal web. Barely a fraction of content available elsewhere. The collection of all these hidden sites is not, as is commonly spouted by governments and many members of the media, several orders of magnitude larger than the normal web.

It's not clear how many people access the dark web on a daily basis, but there's the impression that it's a small number of individuals. The Tor Project claims that only 1.5 percent of overall traffic on its anonymity network is to do with hidden sites, and that 2 million people per day use Tor in total.

In short, the number of people visiting the dark web is a fraction of overall Tor users, the majority of whom are likely just using it to protect their regular browsing habits. Not only are dark web visitors a drop in the bucket of Tor users, they are a spec of dust in the galaxy of total Internet users.

It's Not Impenetrable

Finally, the dark web is not some zone beyond the reach of law enforcement. Although Ross Ulbricht is the most famous dark web personality to get busted, he is far from the only one. Over 300 dark-web-affiliated people have been arrested since 2011, according to independent researcher Gwern Branwen.

Dealers of drugs and guns, people who order illegal narcotics, and the staff and administrators of sites have all been successfully apprehended by police. However, this number should be considered as the "lower-limit" Branwen previously told me, because it only includes those arrests that are related specifically to the dark web markets and which are publicly known.

The people who run child abuse websites or produce illegal material are also being arrested. In October 2014, a Brazilian dark web pedophile site was seized, and 55 people arrested. Then just last month Australian police went public about an operation that had shut down one of the largest child abuse sites in existence.

Just like in the physical world, it turns out that some traditional police tactics, such as going undercover, are incredibly effective against criminals on the dark web.

Should You be Scared of the Dark Web?

Of course, there is a technological space called the dark web, where the servers of websites are hidden behind a veil of cryptography, and users also enjoy strong anonymity protections. But that space is nothing like the fairy tale that has been concocted around it; that of a colossal ocean of digital stores selling exclusive products, where criminals are free from prosecution.

That characterization is not true.

Instead, the dark web is a small collection of sites that reflect the limited number of good, bad, and downright weird humans that use it. Doctors can give impartial advice to drug users, who come out of the woodwork because

of the anonymity awarded to them by Tor; Chinese citizens can discuss whatever they like and circumvent The Great Firewall, and, yes, the dark web is also used to host some seriously depraved sites, such as extreme pornography.

At the moment, the space is probably used mostly for criminal purposes, but its relevance to the world of cybercrime and other domains has been grossly exaggerated.

Looking beyond the scaremongering, however, the dark web actually has promise. In essence, it's the World Wide Web as it was originally envisioned: a space beyond the control of individual states, where ideas can be exchanged freely without fear of being censored.

As countries continue to crack down on the web, its dark counterpart is only going to become more relevant as a place to discuss and connect with each other. We shouldn't let the myth of the dark web ruin that potential.

Cyber Threats and Dangers on the Deep (Dark) Web

The Internet is massive. Millions of web pages, databases and servers all run 24 hours a day, seven days a week. But the so-called "visible" Internet—sites that can be found using search engines like Google and Yahoo—is just the tip of the iceberg.

Below the surface is the Deep Web, which accounts for approximately 90 percent of all websites. As noted by ZDNet, in fact, this hidden Web is so large that it's impossible to discover exactly how many pages or sites are active at any one time.

This Web was once the province of hackers, law enforcement officers and criminals. However, new technology like encryption and the anonymization browser software, Tor, now makes it possible for anyone to dive deep if they're interested.

Defining the Deep/Dark Web

There are a number of terms surrounding the non-visible Web, but it's worth knowing how they differ if you're planning to browse off the beaten path. According to PC Advisor, the term "Deep Web" refers to all Web pages that that are unidentifiable by search engines.

The "Dark Web," meanwhile, refers to sites with criminal intent or illegal content, and "trading" sites where users can purchase illicit goods or services. In other words, the Deep covers everything under the surface that's still accessible with the right software, including the Dark Web.

There's also a third term, "Dark Internet" that refers to sites and databases that are not available over public Internet connections, even if you're using Tor. Often, Dark Internet sites are used by companies or researchers to keep sensitive information private.

While many news outlets use "Deep Web" and "Dark Web" interchangeably, it's worth noting that much of the Deep is actually benign. Everything from blog posts in review to Web page redesigns still in testing to the pages you access when you bank online are part of the Deep and pose no threat to your computer or safety at large.

Access

Most people who wish to access the Deep Web use Tor, a service originally developed by the United States Naval Research Laboratory. Think of Tor as a Web browser like Google Chrome or Firefox.

The main difference is that, instead of taking the most direct route between your computer and the deep parts of the Web, the Tor browser uses a random path of encrypted servers, also known as "nodes." This allows users to connect to the Deep Web without fear of their actions being tracked or their browser history being exposed.

Sites on the Deep also use Tor (or similar software such as I2P) to remain anonymous, meaning you won't be able to find out who's running them or where they're being hosted.

Many users now leverage Tor to browse both the public Internet and the Deep. Some simply don't want government agencies or even Internet Service Providers (ISPs) to know what they're looking at online, while others have little choice—users in countries with strict access and use laws are often prevented from accessing even public sites unless they use Tor clients and virtual private networks (VPNs).

The same is true for government critics and other outspoken advocates who fear backlash if their real identities were discovered. Of course, anonymity comes with a dark side since criminals and malicious hackers also prefer to operate in the shadows.

Use and Misuse

For some users, the Deep Web offers the opportunity to bypass local restrictions and access TV or movie services that may not be available in their local areas. Others go deep to download pirated music or grab movies that aren't yet in theaters.

At the dark end of the Web, meanwhile, things can get scary, salacious and just plain…strange. As noted by The Guardian, for example, credit card data is available on the Dark Web for just a few dollars per record, while ZDNet notes that anything from fake citizenship documents to passports and even the services of professional hit men is available if you know where to look.

Interested parties can also grab personal details and leverage them to blackmail ordinary Internet users. Consider the recent Ashley Madison hack—vast amounts of account data, including real names, addresses and phone numbers—ended up on the Dark Web for sale.

This proves that, even if you don't surf the murky waters of the Dark Web, you could be at risk of blackmail (or worse) if sites you regularly use are hacked.

Illegal drugs are also a popular draw on the Dark Web. Drug marketplace the Silk Road—which has been shut down, replaced, shut down again and then rebranded—offers any type of substance in any amount to interested parties.

You can track - including a DIY vasectomy kit and a virtual scavenger hunts that culminated in the "hunter" answering a NYC payphone at 3 a.m.

Real Risks

Thanks to the use of encryption and anonymization tools by both users and websites, there's virtually no law enforcement presence down in the Dark. This means anything—even material well outside the bounds of good taste and common decency—can be found online. This includes offensive, illegal "adult" content that would likely scar the viewer for life.

80 percent of Dark Web hits are connected to pedophilia and child pornography. Here, the notion of the Dark as a haven for privacy wears thin and shores up the notion that if you do choose to go Deep, always restrict access to your Tor-enabled device so children or other family members aren't at risk of stumbling across something no one should ever see.

Visit the Deep Web if you're interested, but do yourself a favor: don't let kids anywhere near it and tread carefully—it's a long way down.

Placing A Light On The Dark Web

It might sound scary, but the ‘dark web’ is not much different from the rest of the internet

In the wake of recent violent events in the U.S., many people are expressing concern about the tone and content of online communications, including talk of the “dark web.” Despite the sinister-sounding phrase, there is not just one “dark web.” The term is actually fairly technical in origin, and is often used to describe some of the lesser-known corners of the internet.

As I discuss in my new book, “Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P,” the online services that make up what has become called the “dark web” have been evolving since the early days of the commercial internet—but because of their technological differences, are not well understood by the public, policymakers or the media.

As a result, people often think of the dark web as a place where people sell drugs or exchange stolen information—or as some rare section of the internet Google can’t crawl. It’s both, and neither, and much more.

Seeking Anonymity And Privacy

In brief, dark websites are just like any other website, containing whatever information its owners want to provide, and built with standard web

technologies, like hosting software, HTML and JavaScript. Dark websites can be viewed by a standard web browser like Firefox or Chrome.

The difference is that they can only be accessed through special network-routing software, which is designed to provide anonymity for both visitors to websites and publishers of these sites.

Websites on the dark web don't end in ".com" or ".org" or other more common web address endings; they more often include long strings of letters and numbers, ending in ".onion" or ".i2p." Those are signals that tell software like Freenet, I2P or Tor how to find dark websites while keeping users' and hosts' identities private.

Those programs got their start a couple of decades ago. In 1999, Irish computer scientist Ian Clarke started Freenet as a peer-to-peer systemfor computers to distribute various types of data in a decentralized manner rather than through the more centralized structure of the mainstream internet.

The structure of Freenet separates the identity of the creator of a file from its content, which made it attractive for people who wanted to host anonymous websites.

Not long after Freenet began, the Tor Project and the Invisible Internet Project developed their own distinct methods for anonymously hosting websites.

Today, the more commonly used internet has billions of websites—but the dark web is tiny, with tens of thousands of sites at the most, at least according to the various indexes and search engines that crawl these three networks.

A More Private Web

The most commonly used of the three anonymous systems is Tor – which is so prominent that mainstream websites like Facebook, The New York Times

and The Washington Post operate versions of their websites accessible on Tor's network. Obviously, those sites don't seek to keep their identities secret, but they have piggybacked on Tor's anonymizing web technology in order to allow users to connect privately and securely without governments knowing.

In addition, Tor's system is set up to allow users to anonymously browse not only dark websites, but also regular websites. Using Tor to access the regular internet privately is much more common than using it to browse the dark Web.

Moral Aspects Of 'Dark' Browsing

Given the often sensationalized media coverage of the dark web, it's understandable that people think the term "dark" is a moral judgment. Hitmen for hire, terrorist propaganda, child trafficking and exploitation, guns, drugs and stolen information markets do sound pretty dark.

Yet people commit crimes throughout the internet with some regularity—including trying to hire killers on Craigslist and using Venmo to pay for drug purchases. One of the activities often associated with the dark web, terrorist propaganda, is far more prevalent on the regular web.

Defining the dark web only by the bad things that happen there ignores the innovative search engines and privacy-conscious social networking – as well as important blogging by political dissidents.

Even complaining that dark web information isn't indexed by search engines misses the crucial reality that search engines never see huge swaths of the regular internet either—such as email traffic, online gaming activity, streaming video services, documents shared within corporations or on data-sharing services like Dropbox, academic and news articles behind paywalls, interactive databases and even posts on social media sites. Ultimately,

though, the dark web is indeed searchableas I explain in a chapter of my book.

Thus, as I suggest, a more accurate connotation of “dark” in “dark web” is found in the phrase “going dark”—moving communications out of clear and public channels and into encrypted or more private ones.

Managing Anxieties

Focusing all this fear and moral judgment on the dark web risks both needlessly scaring people about online safety and erroneously reassuring them about online safety.

For instance, the financial services company Experian sells services that purport to “monitor the dark web” to alert customers when their personal data has been compromised by hackers and offered for sale online.

Yet to sign up for that service, customers have to give the company all sorts of personal information—including their Social Security number and email address—the very data they’re seeking to protect. And they have to hope that Experian doesn’t get hacked, as its competitor Equifax was, compromising the personal data of nearly every adult in the U.S.

It’s inaccurate to assume that online crime is based on the dark web—or that the only activity on the dark web is dangerous and illegal. It’s also inaccurate to see the dark web as content beyond the reach of search engines.

Acting on these incorrect assumptions would encourage governments and corporations to want to monitor and police online activity—and risk giving public support to privacy-invading efforts.

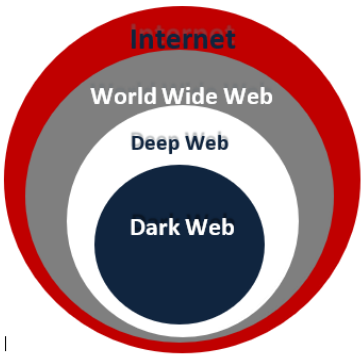
Disturbing Secrets Of The Deep And Dark Web

The Surface Web

The billions of accessible websites on the internet today seem to be overwhelming for a common man. What's more surprising is that these surface websites are about 7-10% of the entire internet. They make up the surface web. The bulk of the internet is hidden in what's called the deep web, or in more depth, the dark web.

The visible World Wide Web with its billions of publicly accessible websites are those which appear on the search engines when searched through some keywords.

These are accessed through web crawler, the meta search engine responsible for merging, interlinking and ranking search results of searching platforms on the surface web. It keeps track of all the websites and links to their webpages, found on the surface web and ranks them according to their content, hence organizing them into an index.



Understanding The Deep Web

One step deeper into the ocean of internet lies the deep web. Websites on the deep web prevent indexing by search engines. Web crawlers are not allowed to access these websites or gather public links from them. These sites are either intentionally made inaccessible or are hidden due to their nature. Several methods are used to prevent their indexing.

The linking of their webpages on surface websites or search engines is disabled by the owners, so they cannot be found through search engines. Access to them can also be denied technically, limiting access using captcha. These websites require a user to log in for accessing any page.

For example, large amount of content on PasteBin or GitHub with no links connecting to the source of information, are only accessed through specific search tools. Some other portals created for only specific people and accessed by their credentials only, are also examples of the deep web.

Deeper Into The Deep Web; Finding The Dark Web

Just like the ocean hides mysteries in its depth, the internet hides hideous tales in the depths of the dark web. The dark web is entirely a mystery with every user being anonymous.

Coming to the actual definition, the Dark Web or Dark nets are highly encrypted networks built on top of the internet and can only be accessed by

specialized software. The websites on the Dark web cannot be accessed by common people surfing the surface web.

These unindexed sites are called dark because all of their users are anonymous. This dark web is the most popular platform for supporting illegal activities.

The most well-known example of illegal activity in the dark web is that of the creation of Silk Road by Ross William Ulbricht, known as dread pirate Roberts. Silk road generated $1.2 billion in 2 years and 9 months, mostly by selling illegal drugs along with other illegal activity. It was later dismantled by the federal government of USA in sept. 2013. In the same year, the usership of The Onion Router, the most common network on the dark web, reached 4 million people worldwide.

The Onion Router

These websites are either present on the private networks like Tor (The onion router) or on the peer-to-peer networks like the Invisible Internet Project (I2P) which can be accessed in web browsers as well. The dark web routes traffic over the network with layers of encryption to preserve anonymity of its users.

The dark web is not accessible for a common man. It requires access to a private network to access the dark web. The dark web enforces many restrictions to maintain privacy of its users.

The Onion Router browser first created by the US Navy is one of the most popular browsers used on the dark web to browse anonymously.

How Does Tor Maintain User Privacy?

This highly secure, easy to use, free software is installed in minutes and routes the network traffic through various Tor servers located globally. This

means that if any information packet is intercepted during transmission, it'll only show sender and receiver as random nodes.

Therefore, the dark web looks like a highly charged galaxy of mobile nodes. This routing node mechanism makes it impossible to trace a user's activity on the dark web.

Many sites from the dark web have a top-level domain (TLD), ending at '.onion' rather than the surface web domains like '.com', '.org' or '.gov'. These top-level domains can only be accessed with browsers or apps running on the Tor network, like Orbot or Orfox mobile apps.

Accessing A Darknet

Darknets allow access or penetration in different ways, based on the purpose of their use, like communication or anonymous browsing. They're also differentiated by their level of security, depending on the encryption protocols and the routing they use.

Friend-To-Friend Darknet

Friend-to-friend is a form of peer-to-peer service, which is accessible by a specific ring of IP addresses. Other IPs can be blocked by the owners to hide their presence on the network.

F2F network has enhanced security, having every exchange on the network encrypted with extra preventive layers of coding.

What's Happening In The Dark Web; Sneak Peek

Internet is a flow of information, a huge amount of which is personal information. The surface internet is evolving swiftly. Compared to the size of surface web, the deep web is huge.

Feb 2017 revealed that there were 1.154 billion websites on the surface net.

The Deep web is 4000 times bigger than the surface web and is growing at a rate which cannot be quantized.

The information flowing through the surface web is often attacked, stolen and sold. Medical Records, IDs, photographs, passports, credit cards Credentials, subscription accounts, browsing history, bank account details, everything is being sold in the dark web.

Who buys this information? Umm, it's hard to tell. Hackers, scammers, marketers, competitors. Anyone.

Darknet serves as host to this black market of information. Stolen information is sold and bought there anonymously. Dark web serves as the Easy marketplace to find the right customers for any kind of information.

This is one of the reasons why Cryptocurrencies were readily adopted for illegal transactions, because they hide identities.

Many researchers dived into the depths to seek information regarding the activities going on in the dark web. 6,608 dark websites were crawled in January 2018, including all types of webpages from entertaining to horrifying, and this is what they found.

Contents Of The Dark Web

The dark web deals with all kinds of scams and illicit content. From credit card cloning products to genius bitcoin scams, everything is available for purchase on the dark web, every passing second. Highly disturbing number of child abuse sites and extreme immoral websites were found on the dark web selling private photos and sexual content.

There are 50,000 extremist terrorist groups operating in the dark web.

Moreover, the 60 largest sites on the dark web have a combined data of 750 TB. Surprisingly, this data alone is 40 times larger than the data of the entire surface web combined.

Things You Probably Don't Know About The Deep Dark Web

- A Medical record is sold for $50
- $20-100 are being earned for selling a credit card information
- Your Social security number is worth $1 on the dark web
- Your bank account details can be sold for $1000
- $50 are earned for 500,000 emails
- Mobile malware is sold for $150
- Commercial malware is sold for $2500
- Exploits can be as expensive as $150,000 to millions of dollars

The Monopoly Of The Dark Web

The Dark web has the monopoly of breaching private information of organizations. Therefore, organizations have been paying large amounts of money to safeguard their leaked information found on the dark web.

The number of breaches has gone down whereas the damages caused by each data breach have significantly gone up. In 2017, organizations paid up to $140 for saving each record from violation and misuse.

However, the information sold on dark web is not guaranteed to be legitimate. So, it can be falsely crafted to ruin reputations of organizations. Vendors of the information are rated by buyers to establish some level of credibility regarding what they bring to the table for selling.

The Geography

The usage of The Onion Router for accessing the Dark Web cannot be marked with a geography. No country can be singled out as being responsible for the existence of the Dark web:

The largest percentage of Tor users comes from the USA with a 19.2% usership.

- The Russians make up 11.9% of the Tor users.
- 9% of the Tor traffic comes from Germany.
- Tor entertains 9.2% of the traffic coming from UAE.
- A report by Visual Capitalist claims that 80% of Tor is funded by the US Government.

What Happened to the Silk Road (Popular Dark Web Drug Avenue)

The Silk Road Creator's Life Sentence Actually Boosted Dark Web Drug Sales, Ross Ulbricht, was sentenced to life in prison without parole for running the Silk Road, an unprecedented dark web bazaar for drugs and other contraband.

The judge intended the sentence to serve as a warning to other would-be

internet narcotraffickers. But new research suggests more clearly than ever before that the strategy of making an example of Ulbricht didn't deter Silk Road users. In fact, it appears to have had the opposite effect.

Starting in late 2014, Ladegaard used a software tool he built to trawl what was then the largest Silk Road–style dark web market daily for sales data. He focused on a 10-month window that included the time directly before and after Ulbricht's sentencing, and found that following Ulbricht's sentencing, the site experienced a significant increase in revenue.

The dark web has only grown in the years since the FBI seized the Silk Road's servers and arrested its creator in late 2013. At that time, the site had roughly 12,000 listings, for items ranging from marijuana to ecstasy to heroin to counterfeit documents.

The largest dark web market today, Alphabay, has well over 300,000 listings, including more than 240,000 for drugs alone. It also offers other wares—like weapons and stolen data—that the Silk Road didn't.

In the case of Ulbricht's sentencing, at least, the more common reaction appears to be curiosity, and a sense of impunity, undiminished by Ulbricht's fate. The Silk Road's founder may languish in a New York prison, but his business model continues to thrive.

How to Go Online Anonymously

You may already be familiar with TorBrowser. But the anonymous internet has a lot more to offer.

The sites you're visiting see you as emerging from a random point on the internet and thus can't trace your true IP address or your associated identity.

Many years have passed since a couple of MIT grads and a Navy-funded researcher first built The Onion Router, or Tor, a wild experiment in granting anonymity to anyone online. Today, **Tor has millions of use**rs. The original project has been endlessly hacked on, broken, and fixed again.

While imperfect, it remains the closest thing to a cloak of anonymity for internet users with a high sensitivity to surveillance, without needing serious technical chops. And it's stronger and more versatile than ever before.

Tor protects your identity online—namely your IP address—by encrypting your traffic in at least three layers and bouncing it through a chain of three volunteer computers chosen among thousands around the world, each of which strips off just one layer of encryption before bouncing your data to the next computer.

All of that makes it very difficult for anyone to trace your connection from origin to destination—not the volunteer computers relaying your information, not your internet service provider, and not the websites or online services you visit.

Tor announced an update to its so-called onion services, which use Tor's anonymizing features to hide not just individual people on the web, but servers too, allowing for so-called dark web or darknet sites and other services that can't be physically traced to any locatable computer.

Beyond merely covering your tracks as you visit websites, the new feature has opened Tor up to a new range of applications, enabling a new generation of whistleblowing platforms and new forms of untraceable messaging. Tor's update has made those **onion services** less easily discovered and strengthened their encryption.

Here's how you can use Tor today, whether you want to want to browse controversial sites in peace, or send messages the NSA can't peep.

Web Browsing

The most basic—and by far the most common—way to use Tor is to simply download, install, and run the TorBrowser from the Tor Project's website. Like other Tor apps, it routes all its traffic over Tor, so that you're browsing the web truly incognito: The sites you're visiting see you as emerging from a random point on the internet and thus can't trace your true IP address or your associated identity.

Aside from making government or other targeted surveillance much more difficult, the TorBrowser also functions as a powerful anti-censorship tool for people in countries like Iran and China, since it hides any direct connection to domains like Google, Facebook, and Twitter that oppressive regimes often block.

Be aware, however, that the final computer routing your traffic to a destination website in that three-hop system, known as an "exit node," can see all of your activity as you connect to a website, even if it doesn't know *where* that activity comes.

Privacy experts warn that law enforcement, intelligence services, and malicious hackers run their own exit nodes for exactly that surveillance purpose. It's critical, then, for Tor users to only visit HTTPS-protected websites to ensure that the information that passes between the browser and the site remains encrypted.

Some popular websites have now even started to run their own Tor onion services, including Facebook and Pro Publica. That means they're essentially hosting a site on Tor's network, so that you can visit through the TorBrowser

and your traffic remains encrypted all the way to its destination, with no need to trust an exit node.

Messaging

It's easy to route not just your web browsing over Tor, but instant messaging, too. The Tor Project offers a program called Tor Messenger, which allows you to combine Tor with the chat protocols Jabber, IRC, Google Talk, and others. That means your connection to whatever server is running that chat service routes over Tor, so that the server can't in theory identify your IP address or location.

This concludes this book. Scroll down.

AUTHOR CONCLUSION

The commonly known websites available through search engines on the internet are called the surface web. These sites make up only 7% of the entire World Wide Web. The rest of the Internet is a highly encrypted world unavailable for general browsing, called the deep web. A part of this web is used for illegal activities and is thus called the Dark web.

My team and I repeated seveal topics in order to help you retain it – **we always repeat things of interest** that should be ingrained in your mind as the reader. Repeating certain things is done on purpose – it is not an accident.

The Dark web offers absolute anonymity to all of its users. All kinds of sensitive information, malicious software, and illegal content is sold and bought on the dark web.

While crafting security strategies, most organizations are unaware of the existence of the dark net. It's important to consider this huge internet world as a threat factor while strategizing for mitigation of threat factors.

Convenient Links for Your Use:

You can download the TOR BROWSER here.

https://www.torproject.org

Protect Your Privacy Here.

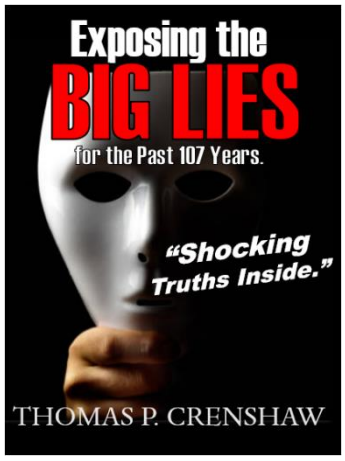
VPN Service

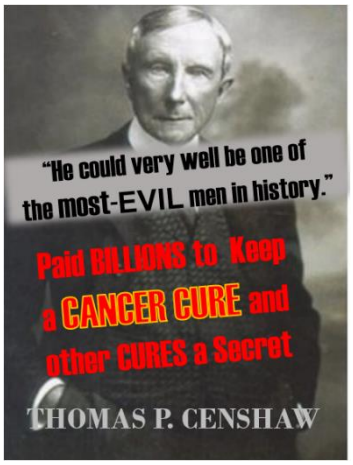
Thank you for your readership. Thomas Crenshaw has authored many controversial books that you will want to know about. Mr. Crenshaw has a great bundle discount available for his fans.

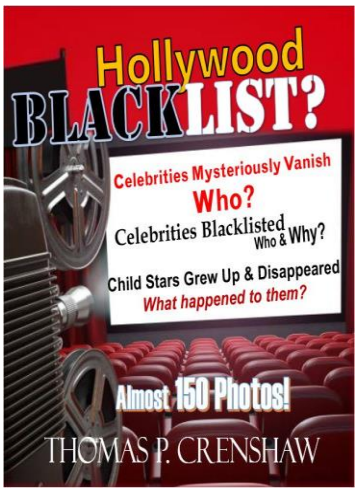
Get more Red Pills here: Join my list.

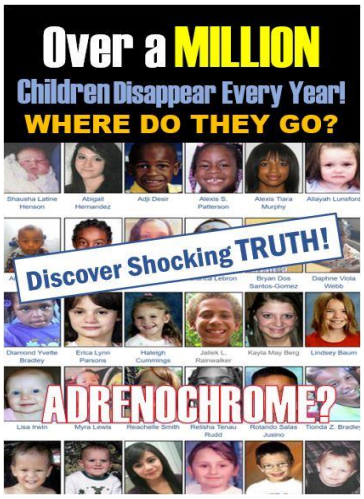
If you benefitted from the information within this book, then please provide a positive review so other will be encouraged to benefit as well. THANKS!

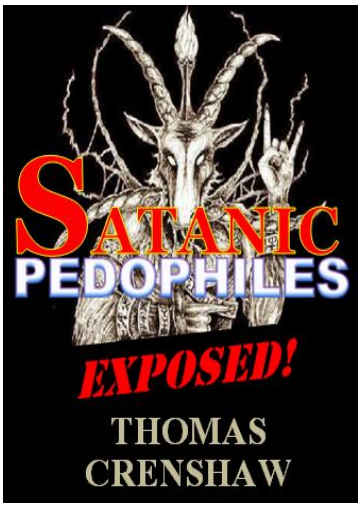
Below are other books that I've authored. I know you'll enjoy any of these titels as well. All available at Amazon. Just click on cover to get more details. THANKS AGAIN!http://amazon.com/dp/B08CD7KCZQ

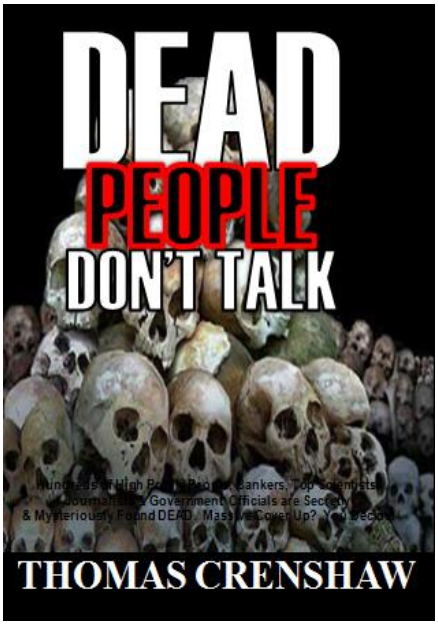





Hollywood
BLACKLIST?
Celebrities Mysteriously Vanish
Who?
Celebrities Blacklisted Who & Why?
Child Stars Grew Up & Disappeared
What happened to them?
Almost 150 Photos!
THOMAS P. CRENSHAW


Over a MILLION
Children Disappear Every Year!
WHERE DO THEY GO?
Discover Shocking TRUTH!
ADRENOCHROME?


SATANIC
PEDOPHILES
EXPOSED!
THOMAS
CRENSHAW


DEAD
PEOPLE
DON'T TALK
THOMAS CRENSHAW