A course by Samuel Champan

Dark Web Course

Cloudwards

The hidden side of the internet has a lot to offer, but every hidden treasure comes with risk.

What’s in the Course?

The dark web: It’s a phrase guaranteed to conjure images of seedy online marketplaces, clandestine criminal activity and even horrific exploitation. However, though all of that can be found on untraceable websites via Tor Browser, the reality is far more complex.

For example, few people know that the U.S. government directly funded the invention of onion routing -- the technology on which the dark web runs -- or that The New York Times, Facebook, ProPublica and other surface websites can be accessed through dark web links.

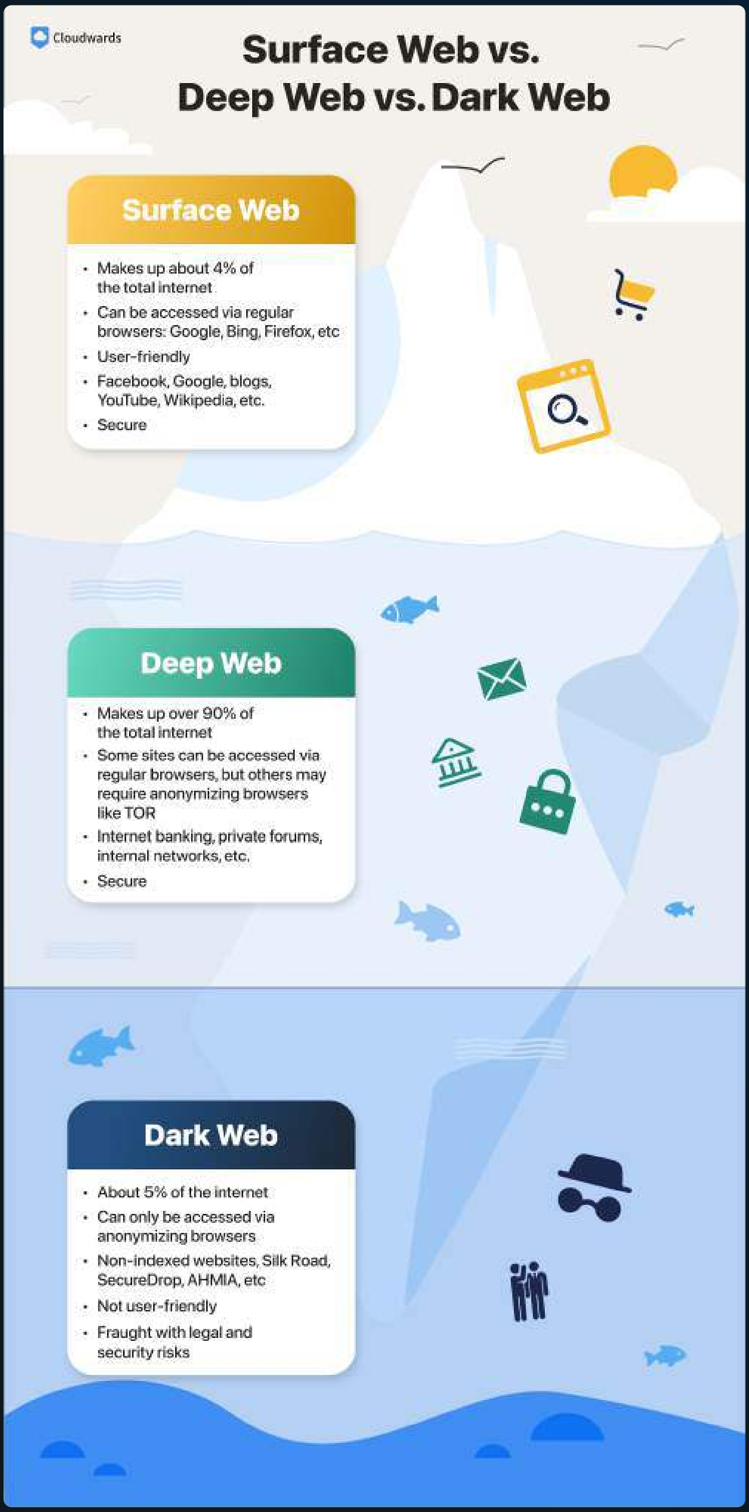
Like any technology, the dark web can be used for good, evil and anything in between. In this course, we’ll explain what the dark web is, what it can be used for and how you can access it without risking your personal security.

After introducing you to vital concepts like Tor, onion links, the Hidden Wiki and the importance of using a VPN, we’ll close with a step-by-step guide on how you can browse the dark web today. Look beyond the myths and discover for yourself what the dark web really is.

SECTION 01

Introduction to the Dark Web: What Is Tor?

First, we must draw a distinction between the **dark web** and the **deep web**. The **deep web** refers to any page that's saved on a web server but cannot be accessed through a search engine.



Surface Web vs. Deep Web vs. Dark Web

Surface Web

- Makes up about 4% of the total internet
- Can be accessed via regular browsers: Google, Bing, Firefox, etc
- User-friendly
- Facebook, Google, blogs, YouTube, Wikipedia, etc.
- Secure

Deep Web

- Makes up over 90% of the total internet
- Some sites can be accessed via regular browsers, but others may require anonymizing browsers like TOR
- Internet banking, private forums, internal networks, etc.
- Secure

Dark Web

- About 5% of the internet
- Can only be accessed via anonymizing browsers
- Non-indexed websites, Silk Road, SecureDrop, AHMIA, etc
- Not user-friendly
- Fraught with legal and security risks

The key trait that most deep websites share is that **they're hidden to preserve access rights, not anonymity**. If you log in to a database, your username and password may be saved; it's also possible to figure out who owns and operates the database. Tor Browser won't help you access any of these sites.

The **dark web** is the small portion of the deep web that is made up of sites using .onion URLs to hide on purpose. A .onion URL makes it impossible to trace which server is hosting a site. Since onion sites can only be accessed through Tor, any visitors are likewise anonymous.

This complete anonymity is responsible for the dark web's shady reputation. Since activity theoretically can't be traced, .onion URLs are the refuge of choice for everything from drug sales to cryptocurrency scams to the sharing of stolen credentials.

However, it bears repeating that not all dark web activity is inherently illegal or malicious. There are many reasons to seek anonymity online. A 2020 study, in which researchers operated one percent of all entry nodes in the Tor network, determined that **only 6.7% of Tor users on any given day** are looking to reach onion sites associated with criminal activity.

In this section, we'll start by explaining in more detail how the deep web and the dark web differ from the surface web. We'll then cover the technology that lets people access the dark web and makes it possible to host websites anonymously. Finally, we'll learn how the dark web has evolved over the years and clear up some common misconceptions.

The Deep & Dark Web vs. the Surface Web

In order to properly understand how the deep web and the dark web work, you first have to understand a few fundamentals of how the regular internet operates, especially as it relates to search engines.

Crawling is the process by which search engines scour the internet for new content and websites. Automated bots known as crawlers start out on websites already known to the search engine and visit every link on these websites. They then do the same for the sites they're led to, and so on. This is the main way that search engines like Google add web pages to their index.

Indexing is the process of storing and categorizing the web pages and sites that the crawler bots find. Sites stored in the index are ranked based on a variety of factors, which decides how far up on the results page the sites appear in a search.

Serving is the final step of the process. The search engine receives a query from the user, finds the most relevant results in the index and then shows the user the resulting web pages.

Now you can start to understand what makes the deep web different. There are three general reasons a site might not turn up on a search engine:

- **Non-indexed:** The website does not exist in a place where search engine crawlers can reach it. Examples include sites that haven't been launched yet, saved drafts not ready for publication or sites whose owners have prohibited crawlers for privacy reasons.
- **Paywalled:** The website is only accessible to those who pay a fee, such as a streaming service content library or a catalog of academic papers.
- **Password-protected:** The web content is secured by a password so only authorized individuals can access it. Most of the deep web exists in password-protected vaults, comprising large databases of potentially sensitive information.

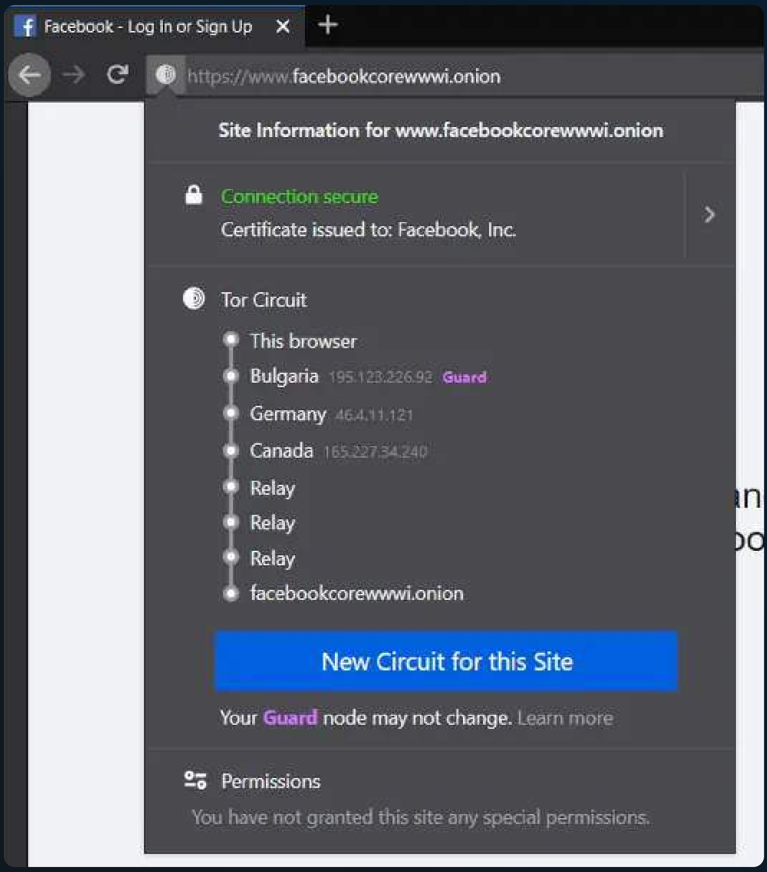
Any site that another surface website never links to will be completely invisible to crawler bots, and thus will never appear as a search result. Therefore, to reach a site on the deep web, you'll need to know its address ahead of time. If it's a dark web site, the URL will end in **.onion**, indicating that it's only reachable via Tor.

Aside from not being indexed, both deep web and dark web sites work the same as surface websites. They're hosted on servers and displayed to end users upon request via web browsers. It's not a separate internet at all -- in fact, some sites have both traditional URLs and dark web onion addresses that display the same content.

How Does the Dark Web Work?

Tor is the technology that makes the dark web possible. Short for "The Onion Router," Tor is a network that routes your internet traffic through a series of volunteer-operated servers to ensure anonymity.

Tor is a free-to-use network of access points called nodes or relays that work like proxies for your connection. It's also the name of the browser you use to connect to this network. When you use Tor Browser, your connection is routed through several of these nodes before arriving at its end destination.


Facebook - Log In or Sign Up
https://www.facebookcorewwwi.onion

Site Information for www.facebookcorewwwi.onion

Connection secure
Certificate issued to: Facebook, Inc.

Tor Circuit

- This browser
- Bulgaria 195.123.226.92 Guard
- Germany 46.4.11.121
- Canada 165.227.34.240
- Relay
- Relay
- Relay
- facebookcorewwwi.onion

New Circuit for this Site

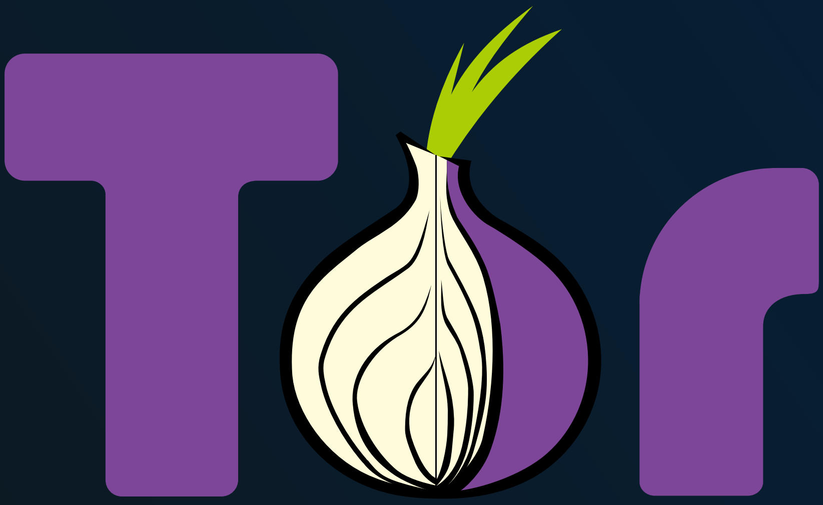
Your Guard node may not change. Learn more

Permissions
You have not granted this site any special permissions.

At each node, your requests and activity are encrypted anew, with each connection after the previous one encrypting the ciphertext it receives. At the final destination, Tor decrypts your connection, “peeling back” the layers of encryption to reach the plaintext inside -- the metaphor that gives onion routing its name.

A nonprofit group called the **Tor Project** operates Tor. Volunteers set up the nodes; anyone who meets the technical requirements can run a Tor relay. This is both a blessing and a curse: It allows for far more nodes than the Tor Project could run alone, but it makes it difficult to vet each node, increasing the potential for a relay to be compromised.

Tor ISN’T USED ONLY TO browse dark web sites, though.



It’s also fundamental to how servers can host sites without those same servers or their visitors being detected. Onion sites, which can only be accessed through anonymizers like Tor, are the dark web’s true dwelling place. We’ll talk more about this in the next section.

The Structure of the Dark Web: Tor, I2P & Other Anonymizing Networks

So far, we've explained how an average user can reach a dark web site. What exactly makes those sites secure, though -- especially if anybody who downloads Tor Browser can find them?

A .onion website, also known as an onion service, is only accessible through its URL. Unlike on the surface web, the URL won't indicate anything about the site itself. Instead, it'll look something like this:

vww6ybal4bd7szmgncyruucpgfkqahzddi37ktceo3ah7ngmcopnpyyd.onion

That string of characters is the unique **public key** associated with the dark web site. Public keys are a vital concept in asymmetric encryption that we won't get into here. For now, you just need to know that a public key can be used to **authenticate** a web server, verifying that it is what it claims to be.

Each .onion URL is connected to a number of **introduction points**, which are specific Tor nodes. These nodes are connected to a predetermined path of other nodes that relay Tor traffic to a specific onion service. The dark web site then uploads an encoded set of descriptors to a Tor database so Tor Browser users can find it.

Users can find dark web URLs through word of mouth, encrypted social media channels or public postings. When you enter an onion address into Tor Browser, you first use the introduction points to verify the destination. You and the website pick a neutral node to act as a one-time **rendezvous point**.

Using the rendezvous point, your device and the dark web server can set up a connection so that layers of anonymity protect both of you the whole time -- like two spies meeting at a third location so neither of their hideouts is compromised.

It's a complex process, but it ensures total anonymity for both users and administrators of an onion service. Tor isn't the only service to make this possible, either; users yearning for anonymity can compare it to other decentralized networks, like **I2P**, **Freenet** and **Hyphanet**.

History and Evolution of the Dark Web

Given that onion routing now has a reputation for abetting illegal activity, it's ironic that it was first developed with funding from the United States government, and still receives about 80% of its money from that source today.

In the 1990s, scientists at the U.S. Naval Research Laboratory (NRL), funded by the Defense Advanced Research Projects Agency (DARPA), created onion routing to protect intelligence communication on the nascent World Wide Web. Despite the work initially being on behalf of the government, NRL made Tor free and open source in 2002.

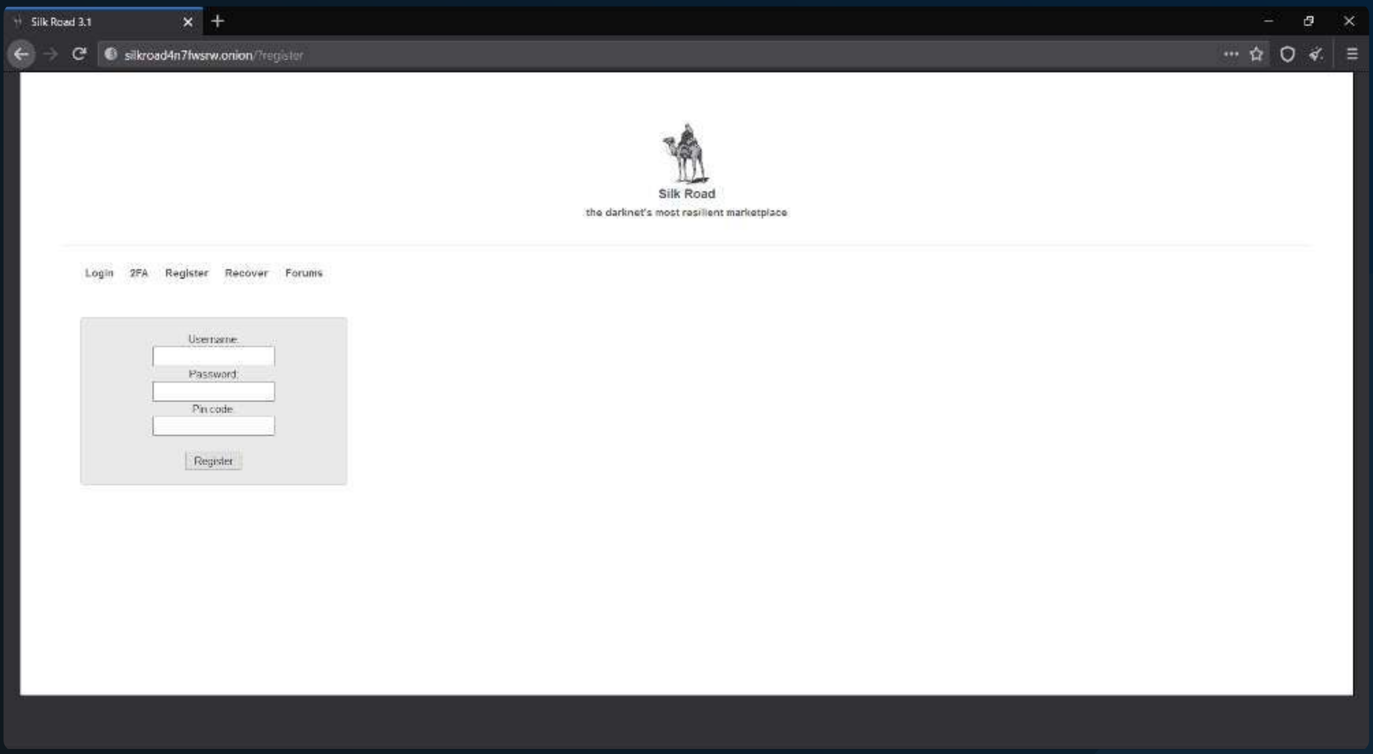
Though that decision may seem counter-intuitive, it makes sense when considering how Tor works. Its anonymous network requires far more people than just the creators to buy in -- Tor is only as good as the number of volunteers willing to run nodes. Also, if it ever got out that U.S. intelligence agents were the only people using the technology, they could be much more easily identified by rival powers.

The Tor Project was founded in 2006 with the goal of maintaining the technology. Tor Browser officially launched in 2008, giving the general public easy access to a completely anonymous internet for the first time. Broad accessibility saw the birth of Tor's reputation for enabling both activism and online crime -- an association that dates from the first appearance of the term "dark web" in print in 2009.

The case of Ross Ulbricht catapulted the dark web to greater prominence. From 2011 to 2013, Ulbricht operated Silk Road, an e-commerce site that was frequently used for buying and selling illegal materials. Despite using onion routing, Ulbricht was eventually unmasked and arrested, due in large part to using his personal email address for Silk Road administrative matters.

The case of Ross Ulbricht catapulted the dark web to greater prominence. From 2011 to 2013, Ulbricht operated Silk Road, an e-commerce site that was frequently used for buying and selling illegal materials. Despite using onion routing, Ulbricht was eventually unmasked and arrested, due in large part to using his personal email address for Silk Road administrative matters.

Using that address, plus Ulbricht's history of making forum posts as himself, FBI agents connected him to the "Dread Pirate Roberts" alias known to run Silk Road. Investigators tracked Ulbricht down in person and confiscated his laptop without him having time to shut it down, providing the key evidence that showed he was in charge. The FBI dismantled Silk Road, but similar sites continue to appear more than a decade later.



The Silk Road case cemented the popular association between dark web sites and seedy crime. There is some truth to this image. Today, .onion sites use cryptocurrency to trade stolen credentials, drugs, weapons, criminal services and illegal pornography. We can't pretend the dark web doesn't enable these things.

On the other hand, plenty of lawful activities are conducted through onion URLs, and many morally upstanding actions (like corporate whistleblowing and popular activism) have reason to remain secret. It's also important to remember that unlawful activity is possible on the surface web as well, though it tends to be a different sort of crime -- scams, stalking and hate speech rather than drug deals.

Finally, never forget that the U.S. government still funds and maintains the Tor Project. This makes a lot of people justifiably reluctant to use Tor, though it's unlikely that the government directly runs enough Tor relays to compromise any individual's anonymity. If such a backdoor existed, it would have been much easier to catch Ross Ulbricht that way than by grabbing his laptop in real life.

Even so, it's important to remember that Tor is a U.S. government project for one reason: Its ability to hide the activity of regular users is a side benefit, not its reason for existing. If Tor ever stopped being a useful tool for intelligence agencies, the government would likely stop funding the Tor project. This should be a reminder to all of us that **Tor should never be anyone's single solution for anonymity**. It's not a silver bullet.

Myths and Realities of the Dark Web

In the final part of this section, we'll unmask common myths and misconceptions about the [redacted], but let's gather them all in one place.

Myth #1: The Dark Web Is Only for Criminals

Accessing the dark web is **perfectly legal**, and a majority of onion services host entirely legitimate content, from informational databases to mirrors of sites on the surface web. The investigative journalism site ProPublica maintains a dark web presence, and even Facebook has a .onion mirror for countries where the main site is blocked.

Remember the two statistics we've shared so far: Not only are fewer than half of onion sites primarily used for illegal activity, but also less than 7% of Tor Browser's daily active users are engaging in criminal acts (though that percentage isn't equal everywhere in the world, and those numbers were gathered in 2020).

Instead, most people who use Tor or go to a .onion site are looking for **privacy and anonymity**. Dark web services host materials banned by repressive governments and provide secure forums for whistleblowers to share information without fear of persecution.

Myth #2: The Dark Web Is Perfectly Safe

We also need to bust the other side of myth #1. Some dark web proponents may tell you that using it carries no risk at all, which is untrue - **you always use Tor at your own risk**.

Tor nodes are run by volunteers who can see your traffic and potentially alter it. Many nodes are malicious and add malicious data to the packets you're sending or receiving. They can also redirect your traffic to a copycat website and steal your login information.

VPN providers such as VyprVPN have consistently asserted that Tor is a subpar solution for true anonymity, and for good reason. For example, Massachusetts Institute of Technology researchers have been able to break Tor without cracking the encryption it uses. Plus, Tor is under constant scrutiny by government agencies because it's often used for cybercrime.

You can circumvent a lot of the inherent issues with Tor by using it in conjunction with a reliable virtual private network (VPN). VPNs encrypt your requests so your ISP and exit nodes can't see that you're using Tor, and they prevent malicious nodes from exposing you or compromising your traffic.

Myth #3: The Dark Web Is 10 Times the Size of the Surface Web

This misconception confuses the dark web with the deep web. In conjunction with myth #1, fearmongers often use it to suggest that the vast majority of the web is used for illegal and immoral commerce.

Instead, **it's the deep web that holds most of the volume, not the dark web**. The deep web is several times larger than the surface web, similar to how a warehouse might be many times larger than a storefront -- most of it isn't meant for public consumption. The vast majority of it consists of databases, drafts and other content unfit for publishing.

At the moment, the dark web consists of about 750,000 unique onion URLs. 3 Bear in mind that only a portion of these represent active websites, so the real number is likely much lower. The dark web is relatively small and partitioned, and it's hard to run a site there for long, especially one providing illegal services.

Myth #4: The Dark Web Is Completely Secure and Untraceable

As Ross Ulbricht's arrest demonstrated, it's entirely possible to take down a dark web site by acting in the real world - Tor won't protect you from poor operational security choices, like using an email address containing your real name.

There are also ways to directly crack Tor traffic. A researcher at Columbia University managed to identify Tor users by setting up a fake website and exploiting a common vulnerability found in home routers. It would take nation-level resources to use that method for long, but some nations are interested in doing just that. It's another good reason to connect to a VPN before using Tor Browser.

In the second section, we'll focus on security preparations you should implement before connecting to the dark web. Whether you're concerned about cybercriminals or government surveillance, Tor's built-in security isn't enough to protect you.

SECTION 02

Dark Web Security

The average user faces threats from both directions on the dark web. **Both law enforcement agencies and criminals can compromise Tor nodes**, a fact that the Tor Project itself admits. To stay safe, you need to take additional precautions beyond what Tor provides.

Nothing illustrates this risk better than the KAX17 incident. For at least a year between 2020 and 2021, a rogue individual or group known as KAX17 operated dozens of Tor relays, seemingly attempting to flood the Tor network with nodes under their own personal control. It's speculated that they might have had nation-level backing, but no one knows for sure.

Though Tor did manage to remove the KAX17 relays, they operated with impunity for a year or more, highlighting the fact that the Tor Project is not set up to detect or punish bad actors. That's to say nothing of the more common exploit in which hackers use exit nodes to launch man-in-the-middle attacks.

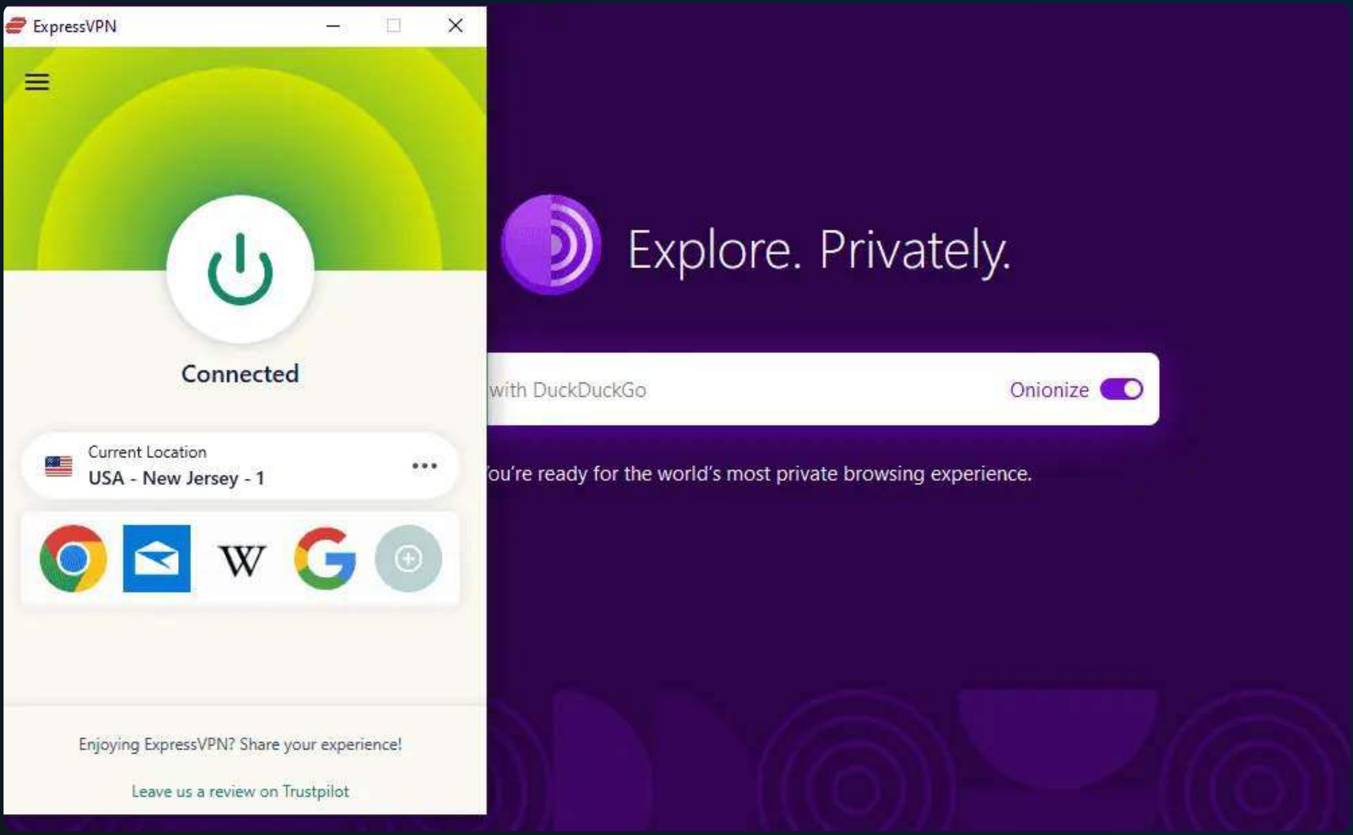
In fact, the risk of compromised nodes is high enough that **many surface websites automatically block any traffic they detect has come from Tor**. This is what makes VPNs such a vital precaution no matter what you do with Tor: A separate encryption source hides your activity not only from malicious nodes but also from your destination server.

Dark Web Security Best Practices

Use these simple common-sense steps whenever you plan to explore the dark web.

Set Up a Secure VPN Connection

All signals sent via Tor are encrypted by default using AES encryption to encode the data itself (both the 128-bit and 256-bit sizes) and RSA-1024 for authentication. Keys are exchanged via TLS. All of these are currently considered secure for Tor's purposes; however, they still leave you vulnerable at the entry and exit nodes.


ExpressVPN
Connected
Current Location
USA - New Jersey - 1
Enjoying ExpressVPN? Share your experience!
Leave us a review on Trustpilot
Explore. Privately.
with DuckDuckGo
Onionize
ou're ready for the world's most private browsing experience.

Remember that Tor Browser sends your traffic through a maze of volunteer-run nodes (servers). Though the onion websites you visit don't receive any details about who you are, the Tor entry node does. If a bad actor or an authority figure is running the entry node, they may be able to trace dark web activity back to you.

Using a VPN, you'll be protected from the moment you enter Tor's radar by the same cutting-edge encryption protocols as Tor itself. We recommend picking a VPN with access to WireGuard or OpenVPN, the two VPN protocols that are both open-source and capable of using the strongest encryption technology.

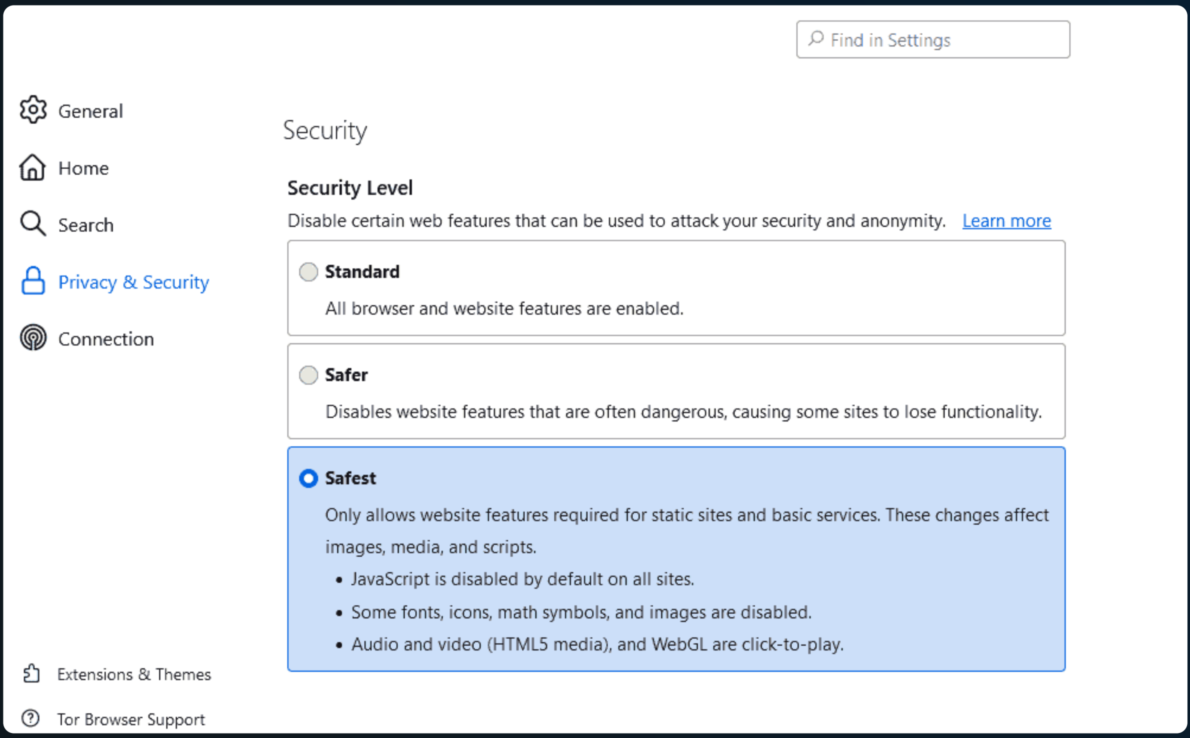
When choosing a VPN for the dark web, pick one that prioritizes security and privacy. Other features, such as speed and unlimited data, may also be important, especially if you want to engage in speed-intensive activity on the dark web. Here are some simple selection criteria:

- **Security:** Make sure the VPN has a kill switch, solid VPN protocols like OpenVPN and WireGuard, and no DNS leaks. The best dark web VPNs also offer advanced security tools such as multi-hop routing and obfuscation so restrictive regimes don't notice when you're using a VPN.
- **Privacy:** Pick a VPN that prioritizes users' privacy. The best VPNs adhere to strict no-logs policies and have independent audits and diskless servers to back up their claims.
- **Speed and data:** If you need to download large files, go with a VPN that speed-tests well and has servers near your physical location.

In Section 5, we'll share a detailed step-by-step guide on how to use a VPN to browse the dark web safely. Make sure you read it closely before doing anything on Tor.

Set Tor's Security to Maximum

Tor Browser comes with three security settings: "**standard**," "**safer**" and "**safest**." "**Standard**" has the full encryption but enables all website features by default. "**Safer**" disables JavaScript on all sites not protected by HTTPS and blocks some other features that commonly leak. "**Safest**" disables all JavaScript functionality and blocks most media by default.



Security

Security Level

Disable certain web features that can be used to attack your security and anonymity. Learn more

○ **Standard**
All browser and website features are enabled.

○ **Safer**
Disables website features that are often dangerous, causing some sites to lose functionality.

● **Safest**
Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.
- JavaScript is disabled by default on all sites.
- Some fonts, icons, math symbols, and images are disabled.
- Audio and video (HTML5 media), and WebGL are click-to-play.

"Standard" is sufficient for browsing on the surface web, but on the dark web, **you should always set your Tor security to "safest."** Legitimate onion sites are built without frills, so they don't contain any elements that might expose you to risk. They should function fine, even on "safest" mode.

Do Not Click Unknown Links

Since all dark web sites are reached via .onion URLs, **there's no way for you to know for sure where an external link is going**. If you aren't careful, a link could take you to a site that automatically begins downloading malware or that contains abusive sexual content.

The safest way to navigate the dark web is to **follow vetted .onion URLs** to sites you trust and to **remain within those sites' directories**. If you jump too often from one site to another, you could end up anywhere. We'll talk more about safe navigation in Section 3.

Don't Download or Buy Anything

Never forget that dark web sites are completely unregulated and run by people who are mostly (but not always) out of the reach of the law. Anything you download could contain malware.

If you must download a file from a dark web site - even one you trust - **use an antivirus program to place the file in a walled-off sandbox where it can be scanned safely**. This feature comes standard on Microsoft Defender and several other popular antiviruses.

Of course, buying a physical product is even riskier. Sellers on some dark web marketplaces deal in products that don't work as advertised or outright don't exist. After all, if the sellers scam you, it's not like you can find them to complain.

SECTION 03

Navigating the Dark Web

Other than using Tor and a VPN, the most important step to use the dark web safely is to **verify the authenticity of any .onion link before you click it**.

This is harder than it sounds. Because a site's .onion URL is also its public key, you can be sure that every onion link goes to the same authenticated location. However, since onion links don't have proprietary domain names, **it's absolutely possible to pass off one URL as another** - it's simply a matter of social engineering rather than hacking.

The best way to get a trustworthy onion link is to acquire it from a trustworthy source. For a site like DuckDuckGo or ProPublica that's mirroring a surface site, **your best option is to get the dark web link straight from the surface site**.

Otherwise, your best bet is to rely on strength in numbers. Enough people use highly trafficked sources of onion links, such as the Hidden Wiki, that scams are discovered and reported quickly. This is a double-edged sword, as scammers like to mirror those sources, but most have surface sites you can use to get reliable links.

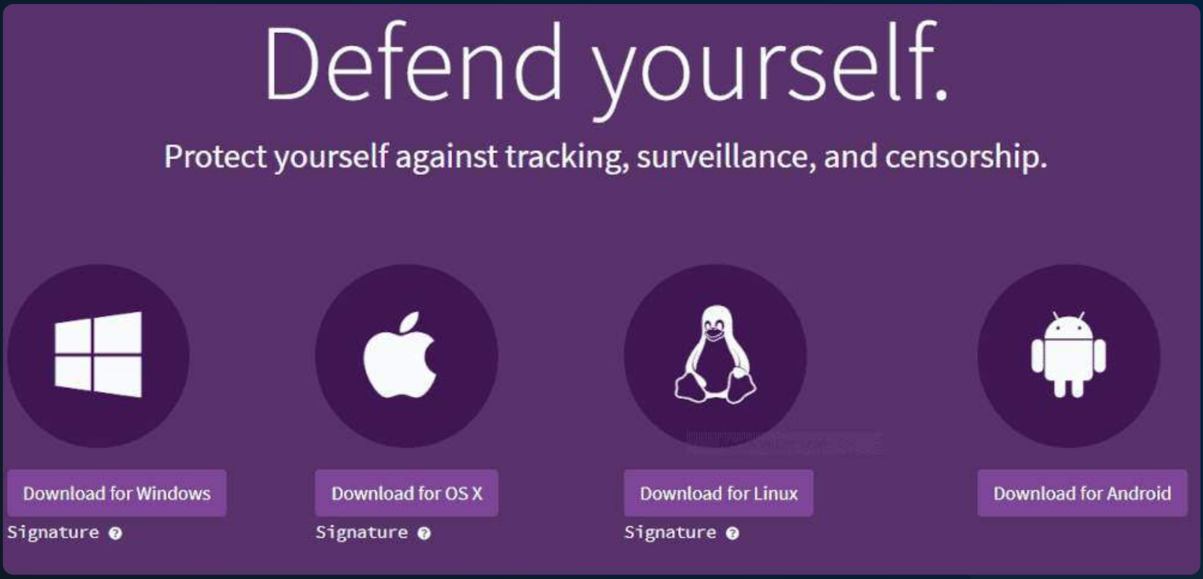
In the end, **you use the dark web at your own risk**. We don't advise visiting any illegal sites, but if you do, you're knowingly placing your online security in the hands of criminals. Tread carefully.

Accessing the Dark Web

Tor is the only way to access any site on the dark web. However, **you don't necessarily have to use the Tor Browser itself**. It's by far the easiest method, but if you really like how your current browser is configured, you have a couple of other options.

Tor Browser

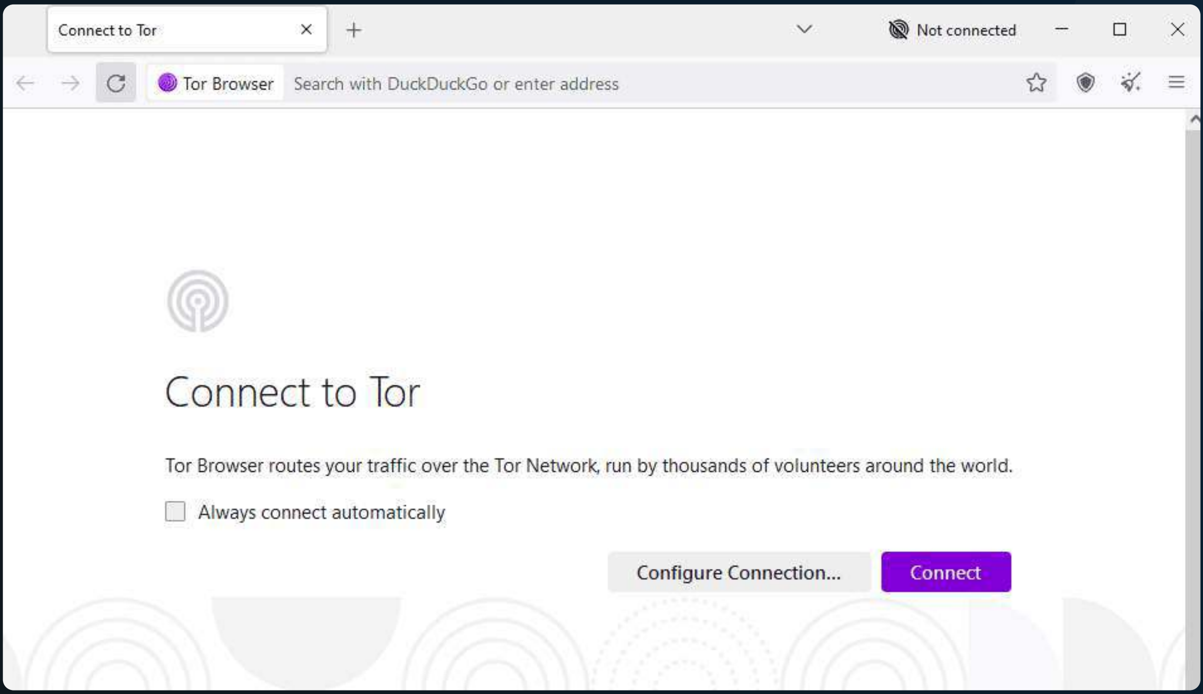
Go to the ⟶ Tor Project's website and **download Tor Browser** for your Windows, Mac, Linux or Android device. If you're on iOS, you can download the Onion Browser app, which the Tor Project endorses.



Defend yourself.

Protect yourself against tracking, surveillance, and censorship.

Double-click the installation file to **install the browser** on your device. If Tor and other anonymizing browsers are blocked in your country, **connect to a VPN first** to circumvent censorship. When you launch Tor Browser for the first time, you'll have the option to set up the Tor network. Click "**connect**" to ensure the browser routes your traffic over Tor relays.



Connect to Tor

Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.

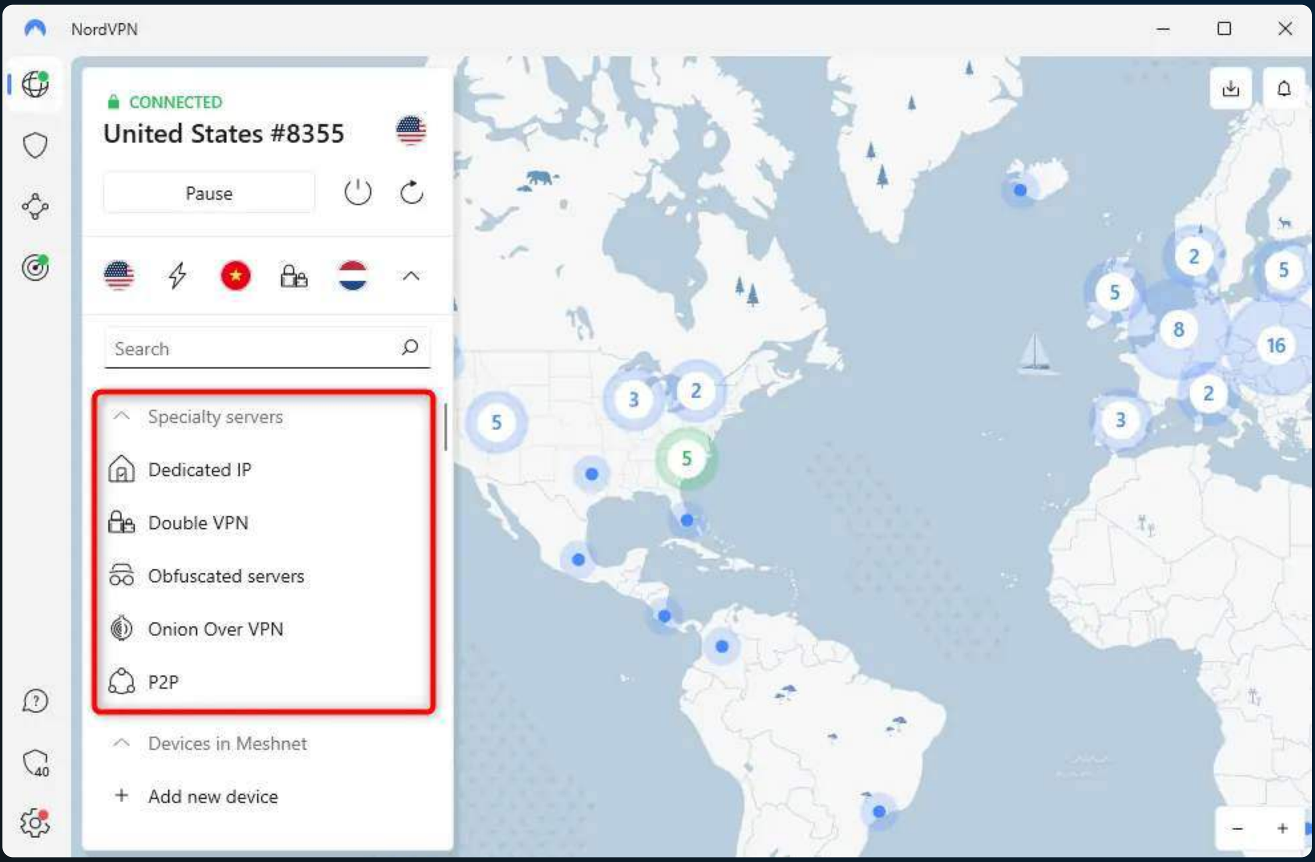
☐ Always connect automatically

Configure the browser's security and privacy settings to the highest levels. At the top right, open the browser's settings and select "**privacy and security**." Configure the browser privacy and permissions to your liking, scroll down to the "**security**" section and set the security level to "**safest**" mode.

If you haven't connected to your VPN yet, **do so now**. All that's left is to find an onion link from a reputable, widely used source. Once you have one, **type the dark web address** into the search bar and press "enter."

Other Browsing Options

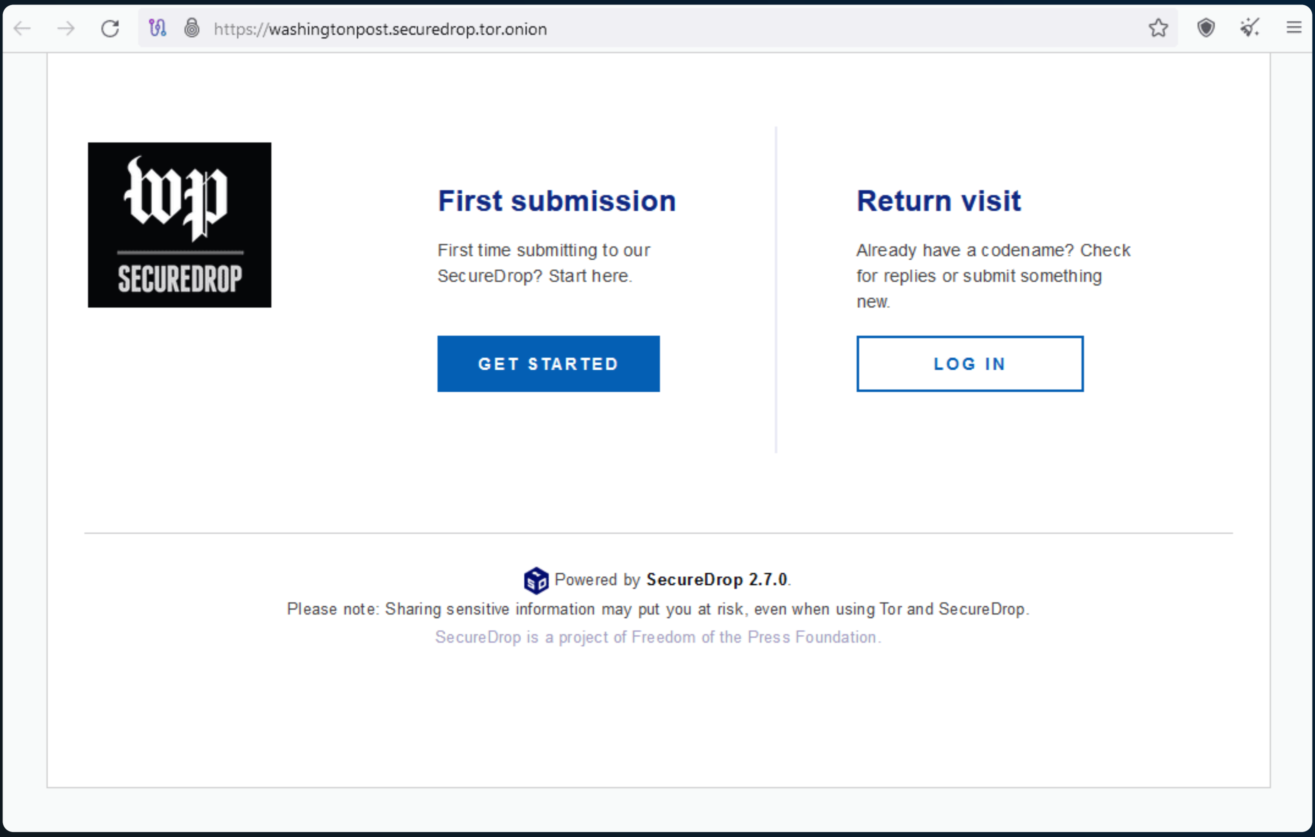
If you'd rather not use Tor Browser itself, your other option is to find another app that's able to use the Tor protocol. For example, **Proton VPN** and **NordVPN** both have servers that let any browser access .onion links. **Brave**, a private browser, has an extension that opens Tor windows, and the Tails private OS uses the Tor network for everything by default.



Popular Dark Web Sites

Before we list any popular dark web sites, a word of warning: The more popular a dark web site is, the more likely scammers are to create a fake version of it and spread the deceptive onion link. Make sure you never click on an onion link without authenticating its source. Remember, **when in doubt, get the link from the mirroring surface site**.

One of the most important and well-known onion services is called **SecureDrop**. This is a document-sharing site that works entirely over Tor, fully obscuring the identity of any sender. News outlets like Al Jazeera, The Guardian and The New York Times have permanent SecureDrop sites set up to receive information from whistleblowers.



https://washingtonpost.securedrop.tor.onion

First submission

First time submitting to our SecureDrop? Start here.

Return visit

Already have a codename? Check for replies or submit something new.

Powered by **SecureDrop 2.7.0**.
Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.
SecureDrop is a project of Freedom of the Press Foundation.

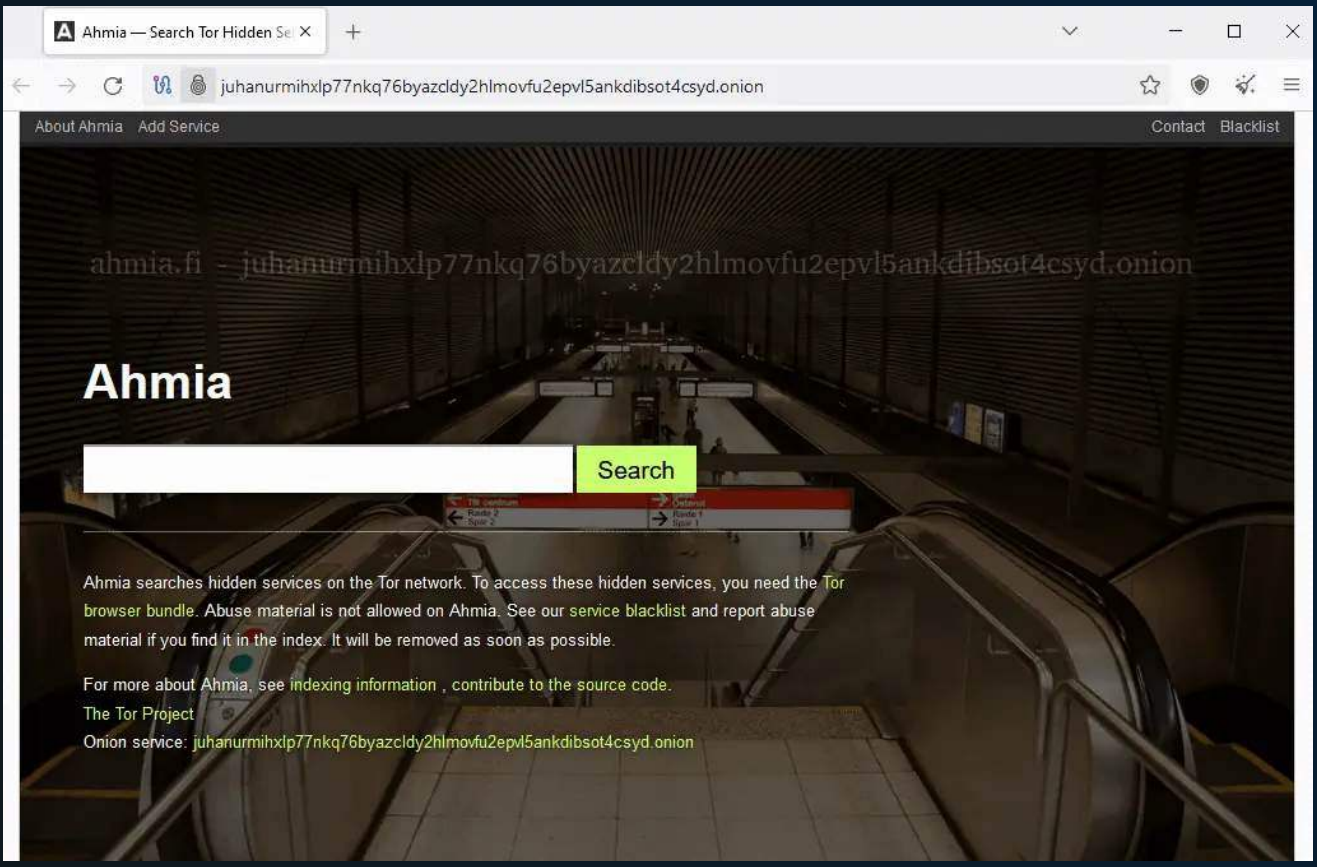
Mail2Tor is another site dedicated to sending and receiving secure messages. Like it sounds, it's an onion-encrypted email site that you can also set up on a desktop client. **Proton Mail**, the well-known secure email client, also has an onion address

Dark Web Search Engines & Directories

The Hidden Wiki is the first site that most dark web novices visit. It's the best way to find trustworthy .onion links. In fact, so many people use it to navigate the dark web that any scammy links tend to be exposed quickly. The Hidden Wiki lists onion services without judgment; you'll find drug markets rubbing elbows with journalism sites in its directories.

If the Hidden Wiki is ever down, which happens, you can get roughly the same information from **OnionLinks.com**.

DuckDuckGo's onion site is the most secure search engine for the surface web, and it stays true to its vow of never logging or exploiting your search history. However, like Google, DuckDuckgo can't present onion links as search results.


Ahmia — Search Tor Hidden Se
juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion
About Ahmia
Add Service
Contact
Blacklist
ahmia.fi - juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion
Search

Ahmia

Ahmia searches hidden services on the Tor network. To access these hidden services, you need the Tor browser bundle. Abuse material is not allowed on Ahmia. See our service blacklist and report abuse material if you find it in the index. It will be removed as soon as possible.

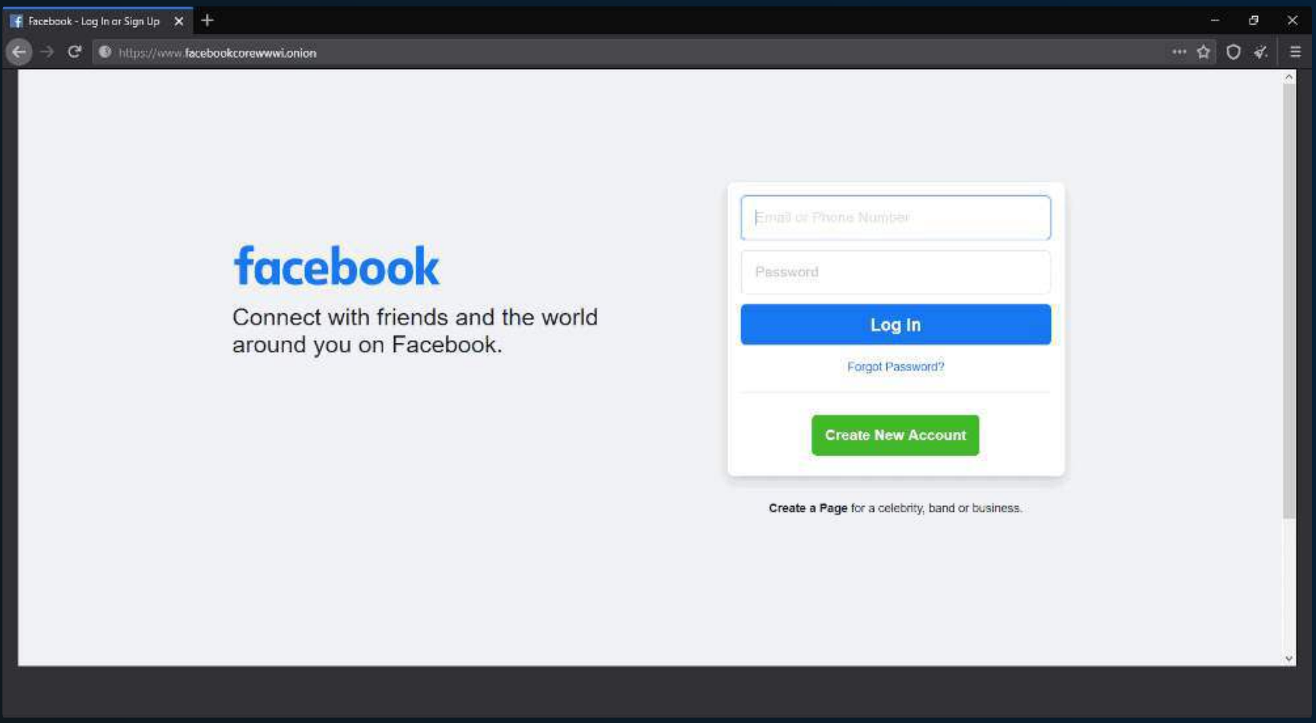
For more about Ahmia, see indexing information , contribute to the source code.
The Tor Project
Onion service: juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion

For a true dark web search engine with .onion links available, try **Ahmia**, which is available on both the surface and the dark web. Ahmia's mission is to make the dark web searchable without ever turning up abusive content. This is laudable, and Ahmia has direct backing from the Tor Project, but it does not promise the same degree of total anonymity as DuckDuckGo.

Another option is **Haystack**, which shares DuckDuckGo's record of not saving user history. Remember to always verify onion links it turns up, since Haystack can't vet them like the Hidden Wiki community can.

Dark Web Forums, Chat Rooms & Social Networks

Facebook has a dark web mirror site that provides a secure connection to its social network. Note that Facebook itself set up the site and still doesn't allow pseudonyms, so it's not exactly anonymous. However, the onion service does make it possible to get on Facebook in countries like China that censor access.



Facebook - Log In or Sign Up

https://www.facebookcorewwwi.onion

facebook

Connect with friends and the world around you on Facebook.

Create a Page for a celebrity, band or business.

Dread is a Reddit alternative for the dark web. Though not a perfect clone, it borrows Reddit's design cues, from the upvote/downvote system to "subdreads" dedicated to specific topics. Subdreads are more likely to focus on explicitly illegal topics than subreddits are, but there are plenty of the same kinds of ordinary fan forums that Reddit hosts.

SECTION 04

Tools and Resources for Browsing the Dark Web

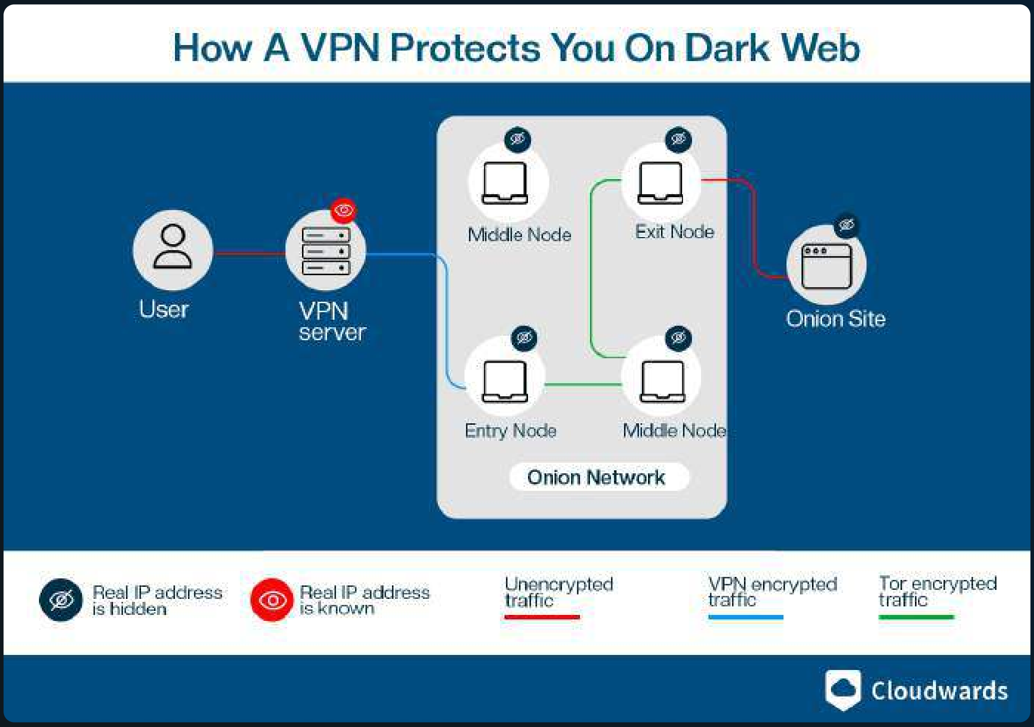
We've mentioned that you should never access an onion service or use Tor without first activating a VPN. In this section, we'll go over VPNs and a range of tools other than Tor that can help you out on the dark web.

VPNs

Why should you use a VPN provider with Tor? First, your internet service provider (ISP) can see that you're using Tor, since the IP addresses of Tor relays are publicly available. Any Tor use is often conflated with entry to the dark web, so your ISP might block or throttle Tor traffic. Some websites block all Tor traffic without exception because of the risk of malicious exit nodes.

Second, Tor sends your traffic through three servers: the guard relay, the middle relay and exit nodes. However, nodes are volunteer-run, and a malicious volunteer could monitor or redirect your internet traffic. A VPN will provide encrypted security for your internet connection.

A reliable virtual private network (VPN)_has features that complement Tor's capabilities and seal its susceptibilities. It encrypts your traffic so your ISP can't see that you're using Tor and prevents malicious nodes from exposing you or compromising your traffic.



A few of the best Tor VPN services include:

- **ExpressVPN**: A highly private VPN whose Lightway protocol improves on WireGuard's speeds without compromising security. Be sure to read our ExpressVPN review.
- **Proton VPN**: Excellent VPN that also offers Tor servers. Learn more in our Proton VPN review.
- **Private Internet Access**: A VPN with a broad server network and P2P compatibility on all servers. Our Private Internet Access Review has more information
- **NordVPN**: A full-featured provider with Onion Over VPN servers that automatically set up a Tor connection. You can learn more in our NordVPN review.
- **CyberGhost**: A user-friendly VPN with secure, locally managed servers in Romania. Our CyberGhost review offers more information.

Security and privacy are the most important considerations when choosing a VPN service. Check each provider's history of responding to leaks and interacting with law enforcement. Speed is also paramount; all five providers above offer lengthy refund periods you can use to test their speeds on the dark web.

Tails OS and VirtualBox

Some VPNs (such as NordVPN and Proton VPN) let you use the Tor network, as do some private browsers (such as Brave). **Tails** goes one step further: It's **an entire operating system** that uses Tor for everything and makes your computer about as secure as a connected device can be.

Tails, which stands for "The Amnesic Incognito Live System," is a Linux distribution. It's free to use but **must be installed on a USB stick** with at least 8GB of storage. Just insert the stick into any computer and reboot the device to start using Tails. Remove the stick and reboot again when you're done.

The key trait of Tails is that **it saves nothing to the hard drive**. If anyone gets ahold of your device, they won't find a trace of anything you did while Tails was active. The USB drive can save some persistent data, protected by a password, but everything else vanishes with each use.

Erasing upon every reboot means Tails is best for short-term uses - generally, **any dark web activity that might leave problematic evidence on your computer**. We don't recommend downloading anything from the dark web until you're more certain you know what you're doing. However, when you're ready, Tails can be a powerful tool.

Tails **automatically blocks any attempt to connect to the internet without Tor**. It comes pre-loaded with Tor Browser and tons of other free privacy tools, including Mozilla Thunderbird, LibreOffice, KeePassXC and OnionShare.

Tails on VirtualBox

If rebooting your computer every time you want to switch to Tails sounds like it would get annoying fast, there's another option: Run Tails in a virtual environment on your normal operating system. You can do this using **VirtualBox**, a free and open-source app that lets you run another operating system in a "sandbox" on the OS you normally use.

The process isn't nearly as technical as it sounds, as both Tails and VirtualBox are available as user-friendly apps. First, **download and install VirtualBox**, then **download the Tails disk image**. Open VirtualBox, create a virtual environment via the **"new" button** and then upload the Tails disk image to it. For more details, skip to Section 5.

If all goes well, you'll be able to run Tails at any time by selecting it from the VirtualBox menu. This makes it much easier to dip into Tails when you want to leave no trace of what you're doing.

OnionShare

OnionShare originated as an app for sharing files between computers using the Tor network. When a user wants to share data, OnionShare creates an ephemeral onion site to host the files. Once the user has sent the files to all the intended destinations, **OnionShare takes down the website**. You can also set up your computer with a persistent onion address to receive files.

Starting in 2019, OnionShare began allowing users to host basic websites on the onion addresses it generated, **becoming the fastest and easiest tool for putting your own site on the dark web**. All you have to do is open a website tag and drag any content into the window. It won't look great, but you can do it with no web design experience whatsoever.

The only catch with OnionShare is that **you need a safe channel to share your onion address with anyone you want to see your files**. Mail2Tor is a good option.

Cryptocurrency

Cryptocurrency is digital money that relies on consensus to determine its value, rather than the authority of a central bank. We won't go too deep into the underlying concepts here, but it's important to know that **cryptocurrency has a symbiotic relationship with the dark web** - most deeply in the case of Bitcoin.

In Section 1, we covered the history of Silk Road, the dark web marketplace for illegal drugs. National currencies were too traceable for Silk Road, so it conducted all its business in Bitcoin.

After Silk Road shut down, the media focused more attention on Bitcoin. Some theorize that this was a factor in the **2017 price boom** that brought cryptocurrency into mainstream relevance.

As that story shows, cryptocurrency and the dark web have grown together, but they first became linked for a different reason: **Crypto makes it easier to hide the identities of the parties in a transaction**. Even if everyone is using Tor and a VPN, any exchange of currency leaves evidence in a centralized bank ledger, which is almost always connected to a real name.

Contrary to popular belief, **crypto is not anonymous**. Instead, most cryptocurrency is **pseudonymous**, replacing each party's name with a fake one. In a crypto transaction, your name is replaced with the numbers and digits of your wallet address. This address is logged on a publicly visible ledger called a **blockchain**, giving the transaction its value.

Though it takes a lot of work, it's possible -- especially with machine learning -- to find the real identity behind a crypto wallet and connect it to illegal transactions. Some criminals have moved away from Bitcoin to currencies like **Monero**, **Bytecoin** and **Zcash**, which have found ways to obscure blockchain transactions.

We do not recommend buying real-world objects on the dark web due to the lack of any product oversight. However, if you wish to do so, **you'll need a digital wallet and some cryptocurrency in hand**.

How to Access the Dark Web Securely: Step-by-Step Guide

Throughout the last four sections, we've given you a detailed overview of what the dark web is and how to access it safely. In this final section, we gather all these guidelines in a single step-by-step reference guide. If you follow these processes in order, you'll be able to discover the dark web on your own terms without risking your safety or anonymity.

Step 1: Install a VPN on Your Router

A VPN masks your real IP address while you use Tor. As long as you **connect to the VPN before opening Tor Browser**, you'll be concealed from malicious node managers, whether individual hackers or government operatives.

We'll be using Tails to get on the dark web, but Tails currently isn't set up to work directly with VPNs. For this maximum-privacy method, your best option is to **install a VPN on your home WiFi router**.

1. Make sure you have a VPN-compatible router. Go to the router manufacturer's website or check the product manual to confirm that it works with third-party router firmware like **DD-WRT, OpenWRT, Tomato or AsusWRT**. Note that most routers that come standard from ISPs are not compatible with VPNs.
2. **Download the proper firmware** onto the router. If you aren't an expert, we recommend hiring someone to do this for you, since improperly changing firmware carries a small risk of rendering your router useless.
3. **Find a VPN that can be installed on routers**. Some good options include **NordVPN, Surfshark and ExpressVPN**. For an even easier time, get **ExpressVPN Aircove**, which comes with the ExpressVPN router app already set up -- so you'll be able to skip the rest of this section. Check out our guide to the best VPN for routers for more information.
4. **Pay** for your chosen VPN and **create an account**.
5. Download a **VPN configuration**. This is a file that contains the information your router needs to connect to a VPN server, including the server's location and the VPN protocol. You can find configuration files on **the VPN's download page**.
6. Open your router's login page by typing the **router's IP address into any web browser's search bar** and hitting "enter."
7. **Enter your WiFi password** to log in to the control panel. **Find the VPN tab**, which will be in different places depending on the router model you're using.

8. **Enable VPN** in the VPN tab. In the boxes that appear, **enter your VPN username and password**.
9. **Import the configuration file you downloaded in steps 1-5**. It should contain all the information you need to finish filling out the form.

Keep your VPN router active until you're finished using the dark web. To disconnect, **disable VPN access from the router control panel**.

Step 2: Set Up a Virtual Machine With Tails

Tails is a highly secret "amnesiac" operating system that doesn't save any data you don't manually designate as persistent. It's the best way to use the dark web without leaving any traces behind on your own device. Ordinarily, you'd have to store Tails on a USB drive, but running it in a virtual environment with VirtualBox is much easier. Here's how to do so.

1. Go to the VirtualBox download page and download the **appropriate app** for your device. Install the **downloaded file** and complete the setup steps.
2. Go to the Tails download page and **download the disk image** for your device. **Don't open or install it** yet. Note that Tails only works on desktop computers, not tablets or phones.
3. Click the **"new"** button at the top of the VirtualBox window.
4. Give your virtual Tails environment a **memorable name**. For the type, select **"Linux,"** then **"Linux (64-bit)."**
5. **Select the amount of RAM you'll borrow** from your main hard drive to run the virtual OS. **One GB** is more than enough for Tails.
6. Click **"create a virtual hard disk now."** For the file type, choose **"VDI (virtual disk image)."** Set the storage to **"dynamically allocated."**
7. **Select a location** on your drive to create the OS, then **choose the default storage capacity**.
8. You should now see your virtual OS appear in VirtualBox. **Right-click on its name** and select **"settings."**
9. In the window that appears, select the **"storage"** tab. **Click the disk icon by "empty"** to open your file explorer. Navigate to the **downloaded Tails disk image** (which should be in your usual downloads folder if you haven't moved it) and **double-click on it**.
10. **Run your new virtual environment**. If you followed these steps accurately, the Tails launch page should appear. Click **"start"** to begin using Tails with the default settings.

Once you've set up your Tails environment, complete all the steps below on Tails instead of on your normal OS. Assume that everything happens in Tails from now on -- we won't keep reminding you. If you need to pause in the middle, shut down the virtual environment and come back later.

Step 3: Download Tor Browser

This step is extremely straightforward. **Tor Browser is packaged with Tails**, so if you downloaded Tails in step 1, you can skip this step. If you'd prefer not to use Tails for any reason, go to the Tor Project download page and **pick the right version of Tor Browser** for your operating system.

In case you can't access the Tor website -- say, if you're in China or another country that blocks it - you can get a download file via **email or Telegram**. For email, send a message to **gettor@torproject.org** and include the OS you're using in the email's body. On Telegram, message **@GetTor_Bot** with the term "/start" and follow the automated instructions.

Configure the browser's security and privacy settings to the highest levels. At the top right, open the browser's settings and select **"privacy and security."** Configure the browser privacy and permissions to your liking, then scroll down to the **"security"** section and set the security level to **"safest"** mode.

Step 4: Use the Surface Web to Find Onion Links

With your VPN router active, the Tails environment running and Tor Browser downloaded, you're finally ready to check out the dark web. **Open Tor Browser**, which works like any other web browser you've used before.

The best way to find destinations is to look for trustworthy onion links on surface web directories, as these are less likely to be malware vectors. Check out the **Hidden Wiki** if you aren't sure where to start; you can get its onion link from its surface page, thehiddenwiki.org.

Step 5: Visit Onion Sites on Tor Browser

Once you have onion links in hand, enter them in Tor Browser's URL bar to connect to the sites. Surf the net as you normally would, checking out whichever corners of the dark web pique your interest.

As you browse, **take extreme care whenever you click on an external link** - anything routing you outside your current directory may take you to a site that executes malware. Fortunately, **Tails automatically equips Tor Browser with uBlock Origin**, which blocks ads and known compromised websites.

CONCLUSION

To wrap up, the dark web consists of sites hosted on onion services, which can only be accessed using Tor Browser. **All you need to browse the dark web is a Tor download and an onion link**. However, to be extra safe, we recommend also using a VPN. If you're working with sensitive information, running a virtual Tails OS environment is a good idea as well.

We hope you've enjoyed our free course on how to use the dark web safely. If you learned something here, we highly recommend checking out the other free and premium courses on Cloudwards. Thank you for reading!

AUTHOR BIO PAGE

writer:
Samuel Chapman

Snapshot

Samuel Chapman is a writer and editor for Cloudwards. His writing and research focus on VPNs, anonymity and online privacy.

Background and Education

Samuel Chapman is a writer and editor at Cloudwards and an expert in online security, privacy and cryptocurrency. His tenure at Cloudwards spans over four years, and he has also written for brands like Koalafi, Ivee and Lunchables, and serves as content manager for PrivacyJournal. Samuel enjoys delivering clear, compelling narratives that demystify complex topics for a broad audience.

As an editor, he uses his keen eye for detail and commitment to high-quality writing to make Cloudwards the best online source for understanding cloud-based technology. Outside of his professional pursuits, Samuel's passions include writing fiction, historical fencing, board games, and hiking.

Samuel holds a Bachelor of Arts in Environmental Studies from Whitman College and a Master of Fine Arts in Creative Writing from the University of Southern Maine.