# DARKNET – A LEGITIMATE ENTITY OR A DOUBLE-EDGED SWORD?

August 22, 2022

## Table of Contents

*Every citizen is entitled to their privacy, but in today's world, it is difficult to use the Internet without getting tracked or monitored in large private and public databases. The dark Web is home to chats, e-mails, and libraries of users who do not want businesses or governments to know what they are doing online. But is it completely safe to do so? We answer all your queries about the Dark web in this piece.*

## WHAT IS THE DIFFERENCE BETWEEN DARKNET, THE DEEP WEB, AND THE INTERNET?

Before we understand the difference between the Internet, the deep Web, and the darknet, let us know what these three terms signify.

- **The Surface Web:** The Internet comprises a network of computers, also known as web servers, through a global network. So, suppose one sets up a website on the Internet. In that case, other users can access it through computers connected to it using Internet Explorer, Google Chrome, Firefox, Microsoft Edge, Bing, etc. This network that you generally access is known as the surface web. Examples of surface web websites include Facebook, YouTube, Google, eCommerce sites, etc.The websites are usually configured under domains, which the user must remember. For example, one domain is www.google.com. When you enter a domain in the web browser, your computer will look for the computer where the website is located. The location of the server is indicated by an IP address. I You can think of the IP address as a house number that uniquely specifies the location of the server. For example, the IP address of Google is 172.217.18.100. Access to the web pages can be unencrypted (displayed in the web browser with https://domain.com) or encrypted (displayed in the web browser with https://domain.com). Because these web pages are visible to everyone, search engines like Google or Bing can also find and index them. If you want to find out who is operating a website, you can query this by means of WHOIS information at the respective domain provider, provided that the owner has given the release of the registration information.
- **The Deep Web:** The Internet has sections one cannot access using the standard search engines mentioned above. They include content like electronic health records, bank statements, chat messages, e-mails, websites hosting government data, paid streaming sites, etc., that require monthly subscriptions. Any website that requires authentication is also not reachable for search engine bots. These sections constitute the deep web. Please note that this content is legitimate and non-criminal. So, the deep Web is akin to a hidden network within the Internet. One example of the deep Web is the paid subscriptions of streaming websites like Netflix or research data that require users to subscribe by paying monthly fees. Online banking is also a component of the deep Web.
- **The dark web:** The Darknet is similar to the Internet, but there are significant differences. Similar to the Internet, the Darknet is only a network of computers (servers) that are connected to each other. Unlike the Internet, however, you can't access the websites with a regular web browser, for example, but with special software like the Tor Browser. This browser can be installed as an app on the PC or mobile device and access to the darknet is achieved within a few minutes. The special thing about software like the Tor Browser, however, is that communication to the server runs completely encrypted over many other PCs. Everything is encrypted – even the IP address of the systems you are communicating with. Because the connection runs over many PCs, you don't know on which server the website you are accessing is located. Therefore, websites can be operated completely anonymously. In contrast to domains on the Internet, the websites also use much more cryptic names. For example, a darknet does not end in .com or similar, but in .onion. Here is an example of a darknet domain (search engine) that can be accessed in the Tor browser: http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/. Compared to the deep Web, the darknet or dark web comprises illegitimate workplaces

teeming with criminal activity. Like the deep Web, standard search engines like Google or Bing cannot access its content, including data like compromised credentials, stolen credit cards, malware, etc. Generally, the darknet is used for criminal activities like cyberattacks, sex trafficking, drugs, malware, prostitution, and a host of illegal activities.

The primary difference between the darknet, the deep Web, and the Internet is that the darknet is full of illegitimate networks that provide anonymity to its users. Regular web browsers cannot access the data on the dark Web. It requires the use of specific browsers built over the standard Internet. While normal users with the proper credentials can access the deep Web, they cannot access the dark Web even accidentally without using specific software.

However, law enforcement agencies can access the darknet to detect illegal activities like money laundering, crypto jacking, trapping cybercriminals, etc. So, all activity on the darknet is not necessarily unlawful. Many people use the darknet for legitimate reasons, for example, political players, journalists, and whistle-blowers who want to remain anonymous.

## WHO CREATED THE DARKNET?

The Onion routing, which is the technology that enables to maintain users' anonymity, was developed 1990s by the U.S. government. The idea was to protect individuals in the intelligence community by allowing them to communicate anonymously.  It also served to protect whistle-blowers' U.S. Navy later patented onion routing in 1998. After onion routing in 2002 the project expanded and was called "the Onion Routing Project", now commonly known as the Tor Project. The Navy would later release the code for Tor under a free license.

Photo by Ludovic Toinel

## DARKNET STATISTICS:

### *WHICH COUNTRIES USE DARKNET THE MOST?*

The top five countries using dark web technologies constitute India at the top with 26%, followed by Russia at 22%. Brazil follows closely behind at 21%, whereas Indonesia and Turkey comprise 20% and 16% of activity.

### *WHAT PERCENTAGE OF DARKNET CONTENT IS ILLEGAL?*

While it is generally considered that darknet content is illegitimate, legitimate activities constitute a significant proportion of darknet activity. Studies show that nearly 57% of darknet websites have illicit conduct. Alternate research shows that 60% of the action on the darknet is illegal.

### *HOW MANY USERS USE DARKNET DAILY?*

The estimated number of darknet users is around 2.5 million globally. It has a market share of 6% of the Internet. The United States of America leads the pack with 34.81% users, with Russia a distant second at 11.46%. Germany is third on the list at 7.16%, with the Netherlands and France making up the top five with 6.92% and 3.29%, respectively. However, India has the most extensive darknet platforms per capita usage globally.

### *HOW BIG IS DARKNET COMPARED TO THE DEEP WEB OR THE INTERNET?*

The deep Web makes up 96% to 99% of the total web usage, with the surface web comprising 1% to 4%. The darknet shares a small segment of the deep Web with a share of around 5% to 6%.

## OTHER INTERESTING STATISTICS ABOUT THE DARKNET

Here are some interesting statistics concerning the darknet.

- India has the most significant per capita usage of darknet platforms. (Source – Statista)
- 84% of category listings on the dark Web are for guns, pistols, and firearms. (Source – RAND)
- It takes an average of 196 days for a leak to be discovered (Symantec). In that time, your credentials are probably already for sale on the dark web. Cyberattack statistics broken down by year show that 2017 had the most data breaches (1,632) in the U.S., but 2018 had the largest number of records breached (446 million).
- More than 50,000 extremist and terrorist groups are present on the dark Web.
- Credit card details are available for as low as $9, whereas payment data is available for around $270. (Source – Positive Technologies)
- The Empire is the largest darknet marketplace with more than 6000 products. (Source – Darknet Lists)
- As per a recent report, data breaches exposed 22 billion records in 2021.

## HOW DOES THE DARK WEB WORK FROM A TECHNICAL POINT OF VIEW? WHAT ARE HIDDEN SERVICES? HOW DO USERS STAY ANONYMOUS ON THE DARKNET?

We have seen that you need a specific browser known as Tor to access the dark Web. Generally, you cannot access it using regular browsers like Google Chrome, Yahoo, Bing, MS Edge, etc., unless you use some particular proxy services or download a special browser(s), like the Tor browser at www.torproject.org. On installing the browser, users can access the dark Web. We use many URLs to access the internet in everyday life, e.g., www.google.com or www.facebook.com, etc. However, dark web URLs generally end with ".onion"  instead of regular URLs like .com, .org, .net, etc., for example, http://sampledarkweburl.onion (please note that ".onion" sites can only be viewed through Tor)

So what happens when you type a URL in your web browser (client) and try to access a website (server) on the internet in your day-to-day life? In a normal web communication between a client and a server, the web browser (client) sends a request to the unique domain name of a web server (server) for web elements (e.g., web pages or images), and after the client request is serviced by the server, the client and server connection is disconnected.

The Tor browser follows a random path of encrypted servers (or computers on the Internet) to connect to the Web without being tracked. It uses Onion routing (a technique used for anonymous communication over a network). In an onion network, messages get masked in layers of encryption that are analogous to layers of an onion. It hides who is using the transport medium to communicate and with whom. Since it heavily relies on encryption, it helps users to stay anonymous.

For example, the Tor browser will display a different IP address to the one you use regularly. Search engines like Torch or Grams can help you navigate the dark Web. But, you will encounter multiple dead ends, 404 errors, and timed-out connections because it's very disjointed. Very few sites get linked to each other, limiting the web search engine's ability to find new websites and web pages. In most cases, it is like the open Internet from the 90s. The Tor network may host various hidden services notorious for criminal and illegitimate activities, including access to illegal drugs, distribution of child pornography, terrorism, prostitution, and sale of weapons.

## WHAT ARE I2P AND GARLIC ROUTING?

I2P appears to offer many of the same advantages as Tor. Both allow anonymous access to websites, both use a peer-to-peer connection structure, and both work with multi-level encryption. However, I2P was designed to offer additional advantages. The main use case of Tor is anonymous access to the public Internet. The fact that data is hidden in the Tor network is really just a side effect. I2P, on the other hand, was designed to be a true dark web. It is a network within the Internet. However, traffic stays within its boundaries. There are very few outbound connections on the I2P network. At its core, I2P performs packet-based routing. This has the advantage that I2P dynamically routes around congestion and interruptions, similar to IP routing on the Internet. This provides a higher level of reliability.

With I2P, network routes are dynamically formed and constantly updated, with each router constantly evaluating other routers and relaying the results. Finally, I2P establishes two independent tunnels for traffic to traverse the network to and from each host, unlike Tor, which establishes a single duplex connection. This has the added benefit that in the event of an eavesdropper on the network, only half of the traffic is exposed. There is also a difference between the I2P and Tor networks at the application level. Tor works by providing a proxy on your local machine. In contrast, I2P is generally used by applications written specifically for the I2P network. These include instant messaging, file sharing, and email.

Once connected to the I2P, you can browse websites, send e-mails, host websites, use blogging and forum software, use decentralized file storage, engage in anonymous chat, etc. On I2P, multiple messages get encrypted together during transmission, which makes it faster and difficult to distinguish between them through traffic analysis. This mechanism is called "garlic routing" and differs from the Tor network's onion routing, as discussed above.

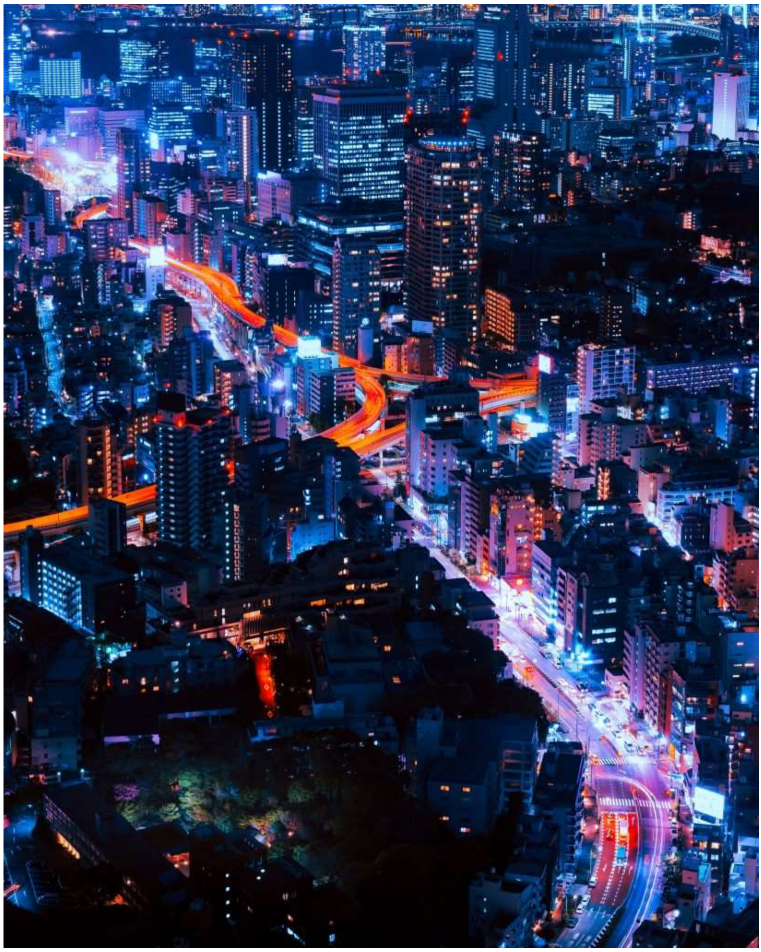

Photo by Pawel Nolbert

## CAN I BE ANONYMOUS AND SURF SOCIAL MEDIA PLATFORMS ON THE DARKNET?

Social media channels are renowned for knowledge and identity sharing. But, the prime quality of the darknet is anonymity. So, the question on everyone's mind is would the darknet has a social media platform? Of course, the darknet has its social media channels. For example, Facebook has an onion address on Tor. The Facebook onion address located at facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion

Similarly, Reddit and Twitter have mirroring websites on the darknet. Reddit is an ideal platform for functioning on the darknet because it offers the values of anonymity and user privacy. Though the social media platforms on the darknet are not as popular as their surface web counterparts, Aether is an excellent social networking site similar to Reddit. Other prominent social media websites on the darknet include TapIIN, BlackBook, TorBook, and Galaxy (1 & 2).

## HOW CAN I SET UP MY SERVER ON THE DARKNET AND OFFER MY SERVICES?

Those who want to set up their anonymous website can create a Tor hidden service site, which runs entirely within Tor. Hence, people can only access it using Tor, and no one can know who made and runs the website. It is possible to install your server and offer services on the darknet. Anyone can set up a web server on the dark web. You can simply download a regular webserver software, which will serve the HTML files and assets like images, etc. (act as a web server). The next step is to download and install the Tor software corresponding to your operating system from https://www.torproject.org/. And, finally, once that Tor's installed and a web server is running, all you have to do is tell Tor about it in some configuration files.

## HOW DO USERS ACCESS THE DARKNET: WHAT ARE THE TECHNICAL POSSIBILITIES?

Users should download and install the Tor browser to access the darknet. It is better to use a VPN. Websites and Internet providers can detect when you use Tor because Tor node IPs are public. Although ISPs can't decrypt your internet traffic and websites can't identify you, they can see that you are using Tor. It can draw unwanted attention and raise suspicions.

Users can also access the darknet using their smartphones. They start by installing the official Android dark web browser, Orbot, available on the Google Play and Tor websites. The Android version is free, whereas iPhone users must pay for an Onion browser.

Users should acclimatize themselves to the darknet by accessing the thehiddenwiki.org website, which offers a list of an extensive range of websites on the Web. Search engines like Torch or Games can also prove helpful. In essence, there are three primary ways to access the darknet:

- ***Tor Browser***: As explained above, by downloading the Tor browser at www.torproject.org
- ***Proxies***: Proxies allow you to access the dark web using regular webbrowsers. There are a few proxy websites, such as, tor2web.org, onion.ws, etc., that acts as a proxy (as a middleman) between hidden dark web services and users trying to access these. The proxy services make dark web services visible to people who are not connected to Tor. In order to access a Tor hidden service you can add a proxy extension to the onion domain, like "onion.to", for example, if the Tor website you wish to visit is "http://sampledarkweburl.onion", you can use a proxy http://sampledarkweburl.onion.to[A1] . Since the .to proxies are not so reliable you can try also the .ws proxies. The hidden wiki for example can be accessed in the darknet using a regular browser with this URL: https://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion.ws/wiki/index.php/Main_Page
- ***Browser Extension:*** Onion Browser Button, TOR Browser Extension are some of the browser extensions that allow you to connect to the Tor network in your browser One example is chrome extension(s), such as the onion search engine.

## WHAT DANGERS ARE THERE WHEN I AM ON THE DARKNET? AM I LIABLE TO PROSECUTION IF I SURF THE DARKNET?

The dark Web can be exciting to browse, but illegal content is readily available because of the lack of proper law enforcement on the darknet. The range includes traumatic child abuse images, child pornography, and even live murders and arson activity.

Browsing the darknet is dangerous because it leaves you vulnerable to cyberattacks if you do not exercise adequate care. As a result, you expose your information systems to malware and, thus, risk the loss of personal credentials. A CISA report discusses how dark web users are prone to identity theft scams.  Besides, you should also note that accessing the dark Web for illicit reasons can lead to criminal prosecution and jail, depending on the local law of the land. Accessing darknet is not generally illegal in various parts of the world, however, how you engage with dark web could fall on either side of legal boundaries. For example, threatening someone, molestation, etc., remain illegal irrespective of you use normal web or darknet. On the other hand, software used to access dark web might be illegal or legal to use based on a specific geographic location. Typically, in countries where online activity is restricted, accessing the dark web is illegal or at least blocked. That includes countries like Russia, China or Iran. You must diligently check your country-specific laws and regulations on surfing the dark Web. Furthermore, visiting the dark net is not a crime unless you look at the child exploitation market or try to sell goods and services illegally.

Photo by note thanun

## WHAT CAN I FIND ON THE DARKNET, AND WHO USES IT FROM A LEGAL VIEWPOINT?

Due to its anonymous nature, the Dark Web is mostly used for illicit purposes. These include buying and selling drugs, passwords, weapons, and stolen data, as well as trafficking in illegal pornography. Several websites hosting illegal stuff have been discovered and shut down by government agencies in recent years. Some of the operators were arrested and served long prison sentences. The anonymity of the dark web has also led to cybersecurity threats and various data breaches in recent decades. For example, there is a brisk trade in stolen data on the darknet, which has been taken in phishing attacks, malware infections, and other hacker attacks. It was the darknet that made electronic cybercrime so popular. In some countries, cybercrime has overtaken traditional crime in the statistics. Link directories like The Hidden Wiki or Daniel can help you get an overview. As mentioned above, the dark Web is full of black marketplaces that sell credit card numbers, drugs, weapons, and even cheap Netflix accounts. Besides, anonymity helps use cryptocurrencies as payment methods. But there are also legitimate reasons to use the dark web.A few people, such as whistle-blowers, might only feel safe contacting journalists (e.g., newspapers, news channels, etc.), or some witnesses may only feel comfortable reaching out to government or law enforcement agencies (e.g., the CIA or FBI, etc.) under a veil of anonymity. Popular websites like BBC, The NY Times, and the CIA also have darker versions on the darknet. Beside regular websites, there are also traditional services offered. The popular e-mail services on the darknet are ProtonMail, Mail2Tor, and C Templar. File uploads and transfer services like SecureDrop, BlackCloud, and MEGATor, help share sensitive information. Journalists and whistle-blowers can use these services to share critical information. Forums and chat boards are also available on the darknet. But, it is not recommended to visit these sites because of the inherent dangers. In these marketplaces,cybercriminals trade phishing data from sites outside darknet sites, e.g., spoofing regular websites and harvesting credentials.

## WHAT ARE CRIMINALS DOING ON THE DARKNET?

The darknet provides the ideal marketplace for compromised credentials, credit card numbers, stolen personal details like e-mail addresses, bank accounts, child pornography, illicit drugs, weapons for terrorism, murder, extortion, and cybercrime. In addition, cyber attack services like access to botnets that cause DDoS attacks are available on the darknet. DDoS or "Distributed Denial-of-Service (DDoS) Attack" is a cybercrime in which the cybercriminal floods a server with internet traffic and prevents the user from accessing connected online websites and services. The dark Web is a place teeming with illegal activities that include child exploitation, Murder for Hire, Blackmail/ extortion, Illegal Drug/ Arms Sales, Sex Trafficking, etc.

## DARKNET AND BITCOIN: WHY ARE THESE TERMS RELATED? HOW DO TRANSACTIONS TAKE PLACE ON THE DARKNET?

People use Digital assets in many areas, including the darknet, as a means of payment for those seeking maximum anonymity when performing operations deemed questionable by the authorities.

Cryptos are popular with sellers of items like illegal weapons, drugs, and other restricted goods. Cryptocurrencies such as bitcoin are used on the darknet because of their pseudo-anonymity for transactions. Such decentralized transactions (which means that no central authority, such as banks, law enforcement, etc., controls or oversees the transactions, and the transactions remain anonymous to some extent) have put limitations on the global intelligence agencies' control over how people transact with one another.

Blockchain is the underlying technology behind cryptocurrencies. Blockchain technology offers decentralization (that means the transactions are distributed on various computer nodes on the internet), and it also provides anonymity (i.e., transactions can not be tracked back to a person). People on the dark net often use cryptocurrencies as a method of payment. Tor browser, on the other hand, provides another layer of security as any transaction that takes place on the darknet is also anonymized by the Tor browser.

Both the users/buyers and service/product providers use dark crypto wallets.

The site operator uses an escrow to hold the payment until the actual product/service has been delivered and confirmed by the buyer and seller. It is done to protect the buyer and sellers from scammers.

## WHAT ARE THE SEARCH ENGINES FOR THE DARKNET? WHAT ARE DARKNET MARKETS?

The Hidden Wiki is one of the most popular choices for dark web searches that acts as a directory of services on the darknet, which is a collection of web URLs or links to other onion sites. Tor's default search engine is DuckDuckGo, and other prominent search engines on the dark web include Torch, Recon, Ahmia.fi, notEvil, Candle, Haystak, Kilos, etc. Haystak has more than 130K searches conducted on its platform daily. The Torch has more than 2M darknet platforms indexed on its database.

A darknet market (DWM) is a commercial website on the dark Web, similar to Amazon or other eCommerce retail platforms, and operates through Tor or I2P. Apart from the fact that many of the products sold on the darknet market are illegal, DWMs operate analogously to mainstream marketplaces. Online Vendors advertise their products on their websites and deliver them to their customers. Buyers choose the product, pay, and the vendor sorts delivery. The DWM holds the money until the customer receives the merchandise and then releases the funds to the seller. Like mainstream online marketplaces, buyers leave reviews for the product and services that help build the darknet vendor's reputation.

## WHY DO ORGANIZATIONS NEED TO CARE ABOUT THE DARK WEB?

Malicious actors are opportunistic characters who try to find the least resistance path. Mostly, they will target smaller organizations because established ones generally have robust cybersecurity controls and safeguards in place. Furthermore, they will attack less security-conscious employees than the key employees of an enterprise, who do not fall prey to their tactics. And they will target services and programs that do not have adequate security controls implemented.

Thus, organizations of all sizes, industries, and locations are at risk of getting targeted, not because of what they do but because they may have made one mistake that allowed the attackers to attack. The dark Web is the digital playground where cybercriminals converge to exchange tactics and methods and buy and sell illicit services and products. An organization may not even know that details of one of its flagship products have been leaked on the dark Web or a pirated copy is being sold for peanuts on the dark Web. Even worse, PII or Personally Identifiable Information of their employees, including C-level executives, is being sold to the highest bidder. Thus, organizations must monitor their digital footprint, making it an essential part of their cyber hygiene and monitoring efforts.

## WHAT IS DARKNET MONITORING?

Dark web monitoring refers to the process by which you can search, track, or monitor the information regarding your organization on the dark web. With the right tools on the dark web, you can track lost, stolen, or leaked information such as intellectual property, compromised passwords, breached credentials, leaked organization's sensitive data, etc. Oftentimes, these sensitive information are usually transacted among unscrupulous characters in the dark web. With proper dark web monitoring tools, you can better detect threats and dangers on the dark web, which is a step further than just anti-virus, anti-malware programs, and programs that help in identity theft monitoring. In the case of these anti-malware and antivirus programs, they help you monitor and prevent any malicious code aimed at stealing information. However, they do very little in situations, where the deed has already been done.

## DARKNET MONITORING: WHO DOES IT?

You can be extremely careful with your web browsing and sharing of content. But is it a guarantee that your credentials cannot be compromised? Surprisingly, it can be. For example, you might share your credentials with your medical service provider or the local supermarket store. Malicious actors can cause data breaches on these servers, access your credentials, and put them up for sale on the darknet. Darknet monitoring can help you by notifying you that your data has been compromised. Private service providers like Kaduu offer darknet monitoring services that monitor various information assets like driver's license number, e-mail address, and mother's maiden name. Bank account details, phone numbers, and credit card information.

Law enforcement agencies as continuously monitor the darknet to identify illegal activity. Journalists keep monitoring the darknet for news scoops. Whistle-blowers monitor the darknet to notify the authorities of scams and other illicit activities. Darknet monitoring is an identity theft prevention process. But, cybercriminals are usually hyperactive on the darknet, monitoring content to launch their nefarious activities.

Photo by Peter Pivák

### HOW SHOULD I MOVE SAFELY ON THE DARKNET?

These tips will help you navigate through the dark Web safely.

- ***Try to use the Tor browser only for accessing the dark Web***
  You cannot access the darknet using regular internet browsers like Google Chrome, Firefox, etc. Instead, you need Tor or I2P. Tor represents a network of volunteer relays for routing the user's internet connection. As it is encrypted and the traffic bounces between various relays, it makes the user anonymous. The Tor browser is free, but we recommend downloading it from the official Tor website. It is also better to download it using your existing browser's incognito settings or a VPN. Tor is officially available on Windows, Android, Linux, and Mac. Using third-party mobile browsers that utilize the Tor network is not advisable.
- ***Use VPN or TOR bridges***
  Though websites cannot identify the user and ISPs cannot decrypt internet traffic on the Tor browser, they can see that it is being used. So, it can generate suspicions and unwarranted attention. Therefore, we suggest using VPN or Tor bridges for accessing Tor. Bridge relays refer to Tor relays that do not get listed in the public Tor directory. It means governments or ISPs wanting to block access to the Tor network can't block all bridges. Thus, Bridges are useful for Tor users living under oppressive regimesand users who want an extra security layer because they're worried somebody can recognize they are using a public Tor relay IP address.
- ***Take safety precautions***
  Activating the VPN is not sufficient to access the Dark Web safely. One needs to take into

consideration every application that is currently running on their computer. For example, one must close all the apps they have accounts on, like a password manager, storage apps like OneDrive, and streaming applications like Netflix. A prudent choice is to close everything that's not essential when browsing the Dark Web. Additionally, cover the webcam and turn off the location on the device.

These precautions are necessary because applications connected to the Internet, such as Dropbox or other cloud-based ones, communicate with their servers, and if you're using the same channel (i.e., Tor) to use these applications. Someone going through the Tor Network traffic may be able to decipher when you log in or log out of your Dropbox account, and a skilled threat actor may then be able to get his hands on other aspects of your identity.

- ***Check for IP leaks***
  After setting everything up, there's still more one needs to do, checking whether they have any leaks that could reveal personal info. The user needs to check for IP, WebRTC, and DNS leaks. To do it, turn on the VPN and head to dnsleaktest.com. And ipleak.net. There, one can check whether the displayed IP address is real or the one provided by the VPN service.

## FINAL WORDS

From the discussion, it is clear that websites on the dark Web are not always secretive. Some "untraceable"website URLs get openly publicized because people want them to be "findable," for example, drug-related marketplaces. What's kept anonymous is the list of users who accessed the websites and when including their physical location so that their servers are not seized and taken offline by law enforcement agencies.

Thus, the dark Web becomes a double-edged sword – it is considered good when you use it to evade surveillance which many of us think is intrusive. Still, it is bad when cybercriminals use it to avoid detection for committing cyber-crimes, which all of us consider unacceptable. Suppose you want to monitor whether any information related to you was leaked on the darknet. In that case, Kaduu offers AI-driven dark web analysis services that can help you take necessary measures before threat actors can use it to their advantage.