EXPLORING THE DARK WEB

SECRETS FROM AN EX HACKER

By Faisal .j

EXPLORING

THE DARK WEB

SECRET FROM AN EX-HACKER

Faisal .J

Copyright Page

Disclaimer

This book is for **informational and educational purposes only.** The author **does not promote, endorse, or encourage illegal activities.** Readers are responsible for their own actions and should comply with all applicable laws. The content is based on research and personal experiences and is provided **"as is" without warranties of any kind.**

Some images in this book were **AI-generated or sourced from online research.** The text has been edited using AI-assisted grammar tools for clarity. While every effort has been made to ensure accuracy, cybersecurity topics evolve, and some information may become outdated.

First Edition: 2025
Independently Published

For inquiries or permissions, contact:
faisaljalvi0509@gmail.com

Support my work & exclusive content:
Patreon: patreon.com/MuhammadFaisal0317

TABLE OF CONTENTS

Chapter 1

INTRODUCTION TO DARKNET

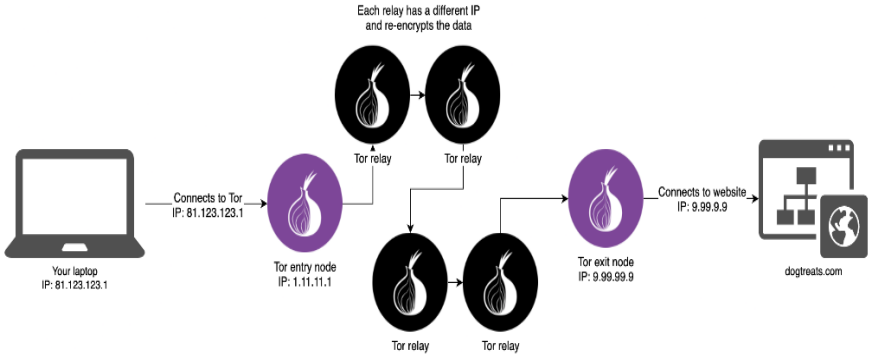
📜**“ "*The Darknet isn't a place you visit—it's a shadowed underworld where secrecy is survival.*"**

The internet has a side most people never see…

TOR (The Onion Router)

Unlike traditional web browsing, where your device directly connects to a website's server, TOR reroutes your

connection through multiple encrypted layers, bouncing your request between different servers worldwide. This process ensures your identity remains hidden, making it nearly impossible.



The First Layer: Entry Point

Your journey into the TOR network begins when you connect to the entry node (Server 1). This node receives your device’s IP address but doesn’t know where you intend to go. It simply encrypts your request and forwards it to another server in the network.

The Second Layer: TOR Nodes

Once inside the TOR network, your request moves through relay nodes (Server 2). These act as intermediaries, ensuring that no single server knows both your identity and your destination. The middle nodes handle encrypted data, meaning they cannot see or alter your request. They only know which node sent them data and where to send it next.

The Third Layer: Exit Node

Your request eventually reaches the exit node (Server 3), the final relay before connecting to the actual website you want to visit. This node decrypts the last layer of encryption and completes the request. However, the exit node still doesn't know the original sender—it only sees the previous TOR relay, maintaining user anonymity.

The Final Destination: Website Server

At last, your request arrives at the web server hosting the content you want to access. From the website's perspective, the request originates from the exit node, not from your actual device. The site has no way of tracing it back to you, ensuring full privacy.

How Data Travels Securely Through TOR

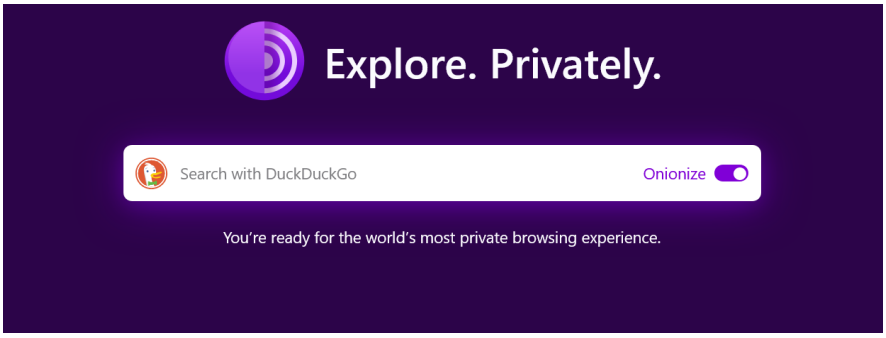
Every piece of information sent through TOR is wrapped in multiple layers of encryption. The process works as follows:

1. Your data is encrypted before leaving your device.
2. The entry node encrypts it again and sends it to the first relay.
3. Each relay node peels away one layer of encryption before passing it forward.
4. Only the exit node sees the final request but doesn't know the sender.
5. This layered encryption method ensures that no individual node knows both the source and the

destination, making it virtually impossible to trace the connection.

Accessing the Darknet with TOR

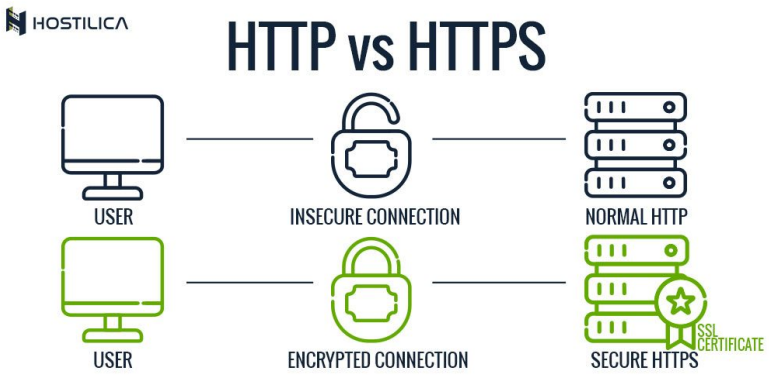
While TOR can be used to browse normal websites, its real purpose is accessing. onion sites hidden services that exist only within the TOR network. These sites cannot be found through regular search engines and require direct knowledge of their addresses. Browsing the Darknet through TOR can be slow, as each request must travel through multiple relays. Additionally, some websites block TOR users to prevent anonymous access. However, despite these limitations, TOR remains one of the most effective tools for protecting online privacy and bypassing censorship.



HTTP vs. HTTPS

Hypertext Transfer Protocol (HTTP) Ahead of the real URL, the abbreviation HTTP looks in the very top from the browser's address bar. The link isn't encrypted. Hackers have a simple time intercepting, manipulating and reading

the information. The TOR browser sets the end to HTTP connections. After entering an HTTP address, the browser asks a securely encrypted HTTPS edition of the webpage. HyperText Transfer Protocol Secure (HTTPS) The URL is preceded by HTTPS and also usually a little padlock icon to signify the safety of their relationship. To boost the safety of HTTP connections, the SSL certificate was added. The computers communicating with each other agree on a frequent secret that the manufacturers of TOR consider HTTP to be so insecure they mechanically join a certificate to every HTTP link, thus transforming it in an HTTPS connection.



Is your consumer completely protected with TOR?

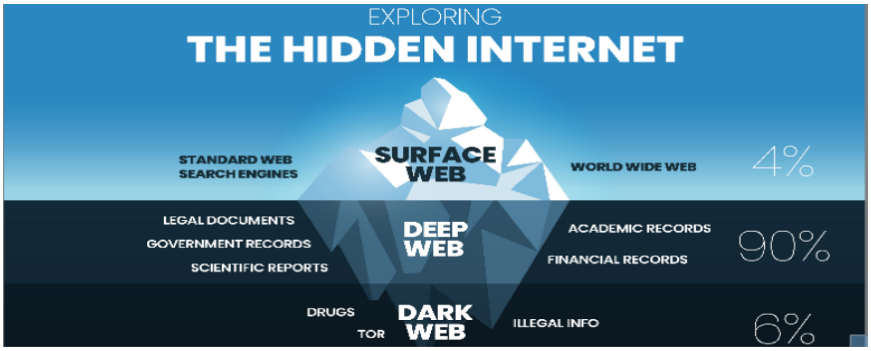
The TOR Browser and similar programs make the avenues taken from the information anonymous. On the other hand, the information sent via it isn't necessarily protected. By way of instance, log-in info, credit card data or addresses could be extracted when inputting data in a web form even when

TOR is utilized. Additionally, the anonymity of TOR communicating may also be eliminated if a person gains access into this TOR browser, which could also be manipulated just like any additional applications. Exactly the same applies, obviously, to servers whereby TOR sends users or about what Deep Web pages are saved. The TOR browser paths a petition Through several nodes. From the perspective of the destination node, this petition comes in the Czech Republic.

Two options to TOR

Though TOR is the best-known way for Anonymizing traffic, it's not the only protocol which may ensure the anonymity of consumers from the deep website. Hornet (Highspeed Onion Routing Network) The anonymization system developed by investigators in the University College London and ETH Zurich is comparable to TOR in performance, but works quicker. I2P (Invisible Internet Project) I2P, on the other hand, functions in principle such as a virtual private network - and is therefore distinct from TOR and Hornet.

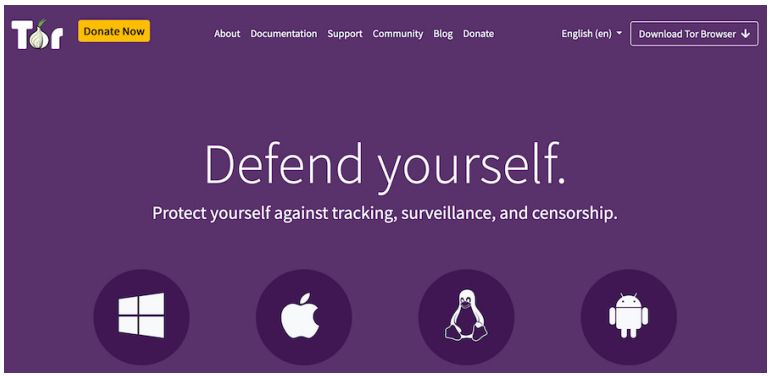
What's the gap between Darknet and Deep Web?



In the most of the favorite German-language networking, the phrases Darknet and Deep Internet are used synonymously. In fact, Darknet and Deep Internet are by no means equivalent since the Darknet is just a little portion of the Internet. Figuratively we could envision the Web such as this: The normal Web, which we could hunt with Google and Co., is the tip of this iceberg. The component under water which we may only see with specific means is that the Deep Web. Along with also the Darknet is the bottom of the iceberg floating in the ocean.

To see the Areas of the iceberg under the surface, special "diving equipment" is needed the TOR-Browser. To get in the Internet to Darknet, more is demanded. While the observable net - i.e. the recognizable, observable and search engine driven Web - is reachable with a typical browser, the profound web operates hidden under the top layer of the network. To access the webpages of the Deep Internet you require collateral, the TOR system, which implies anonymity while browsing. The sole access secret to the Web is a particular software and the proper browser settings.

Who is utilizing the darknet?



Anonymity is especially interesting for two classes: On the one hand, there Are individuals who want the security of the Deep Web because of their own communications. They discuss sensitive information and data and need to fear for their lives or those of the informants if they don't exchange data under the security of the Internet. This group involves the oppressed or dissidents, opposition members out of nations led by dictators or journalists and whistleblowers. Throughout the Deep Web

Anonymization helps journalists shield their resources. By Way of **Example**, Arab Spring activists have managed to get social networking stations throughout the TOR system and disseminate information regarding the revolution. Whistleblowers like Edward Snowden additionally use the Internet to deliver sensitive data to the general public. This original class protects itself from unwanted effects and persecution by visiting the Web. And the next group also utilizes the anonymity of the Deep Web to escape Negative

effects and escape prosecution. This group consists of individuals whose actions on the observable Web would very quickly result in complaints, penalties and imprisonment. Darknet includes forums, internet stores and trading platforms for both goods and services which are either prohibited or subject to strict regulations.

Chapter 2

ACCESSING THE DARKNET

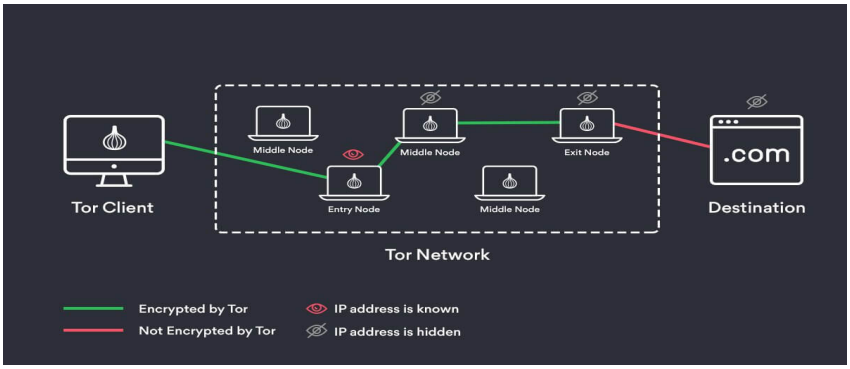
📜“ "***Beyond the indexed web lies a digital abyss, where knowledge and danger walk hand in hand.***"

The Darknet is not just a hidden corner—it’s an entire digital underworld.

The internet has become a fundamental part of running a business. Whether checking emails, staying updated with industry news, or accessing customer data, we rely on it

daily in various ways. But do we truly understand how it works, even at a basic level? Before diving into the darknet and dark web, it’s important to first understand the structure of the internet itself.

The term "Internet" is short for "internetwork," a system that connects multiple computer networks. This interconnection allows devices to communicate with each other, forming the vast, global network we use today. The Internet once capitalized to distinguish it from other internetworks is the most well-known example. It connects billions of devices worldwide through standardized protocols that enable seamless data exchange. While browsing websites is the most common way people use the internet, it’s not the only method of communication. Email, instant messaging, and file transfers (FTP) are other ways information is shared across this network. It’s essential to note that the internet and the web are not the same. The web (or World Wide Web) is just one way to access information on the internet. In simple terms, the internet is the infrastructure, while the web is a service that operates on it.

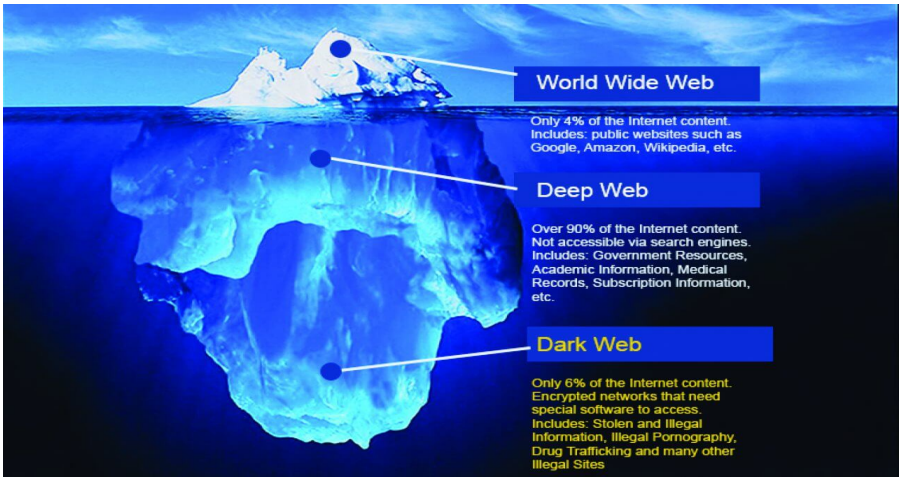


The Surface Internet

The websites we visit daily make up only a small fraction of the entire internet. This portion, known as the surface web, includes all publicly accessible sites that search engines like Google and Yahoo can index and display in search results. While estimates vary, experts agree that the surface web accounts for only about 4% of all online content. If you're curious about how search engines crawl and index web pages, Google's comprehensive guide provides a great overview.

Beyond the Surface

Beyond the surface web lies the vast, hidden world of the deep web and the darknet, which together make up the remaining 90% of online content.



THE DARKNET - THE DARK WEB The Deep Web

The deep web consists of content that cannot be found or directly accessed through standard search engines like **Google or Yahoo**. Examples of deep web content include sites requiring login credentials (such as email or banking portals), unlinked websites that need a direct URL to access, and databases that intentionally restrict search engine crawlers. In fact, a vast majority of deep web content exists in databases that house sensitive or structured information. Many deep web databases have their own internal search functions, allowing users to retrieve information stored within them.

Government databases, personal records, and library catalogs are just a few examples of deep web repositories. Some of these databases are accessible without login credentials, but others require user authentication. Take, for instance, the Denver Property Taxation and Assessment

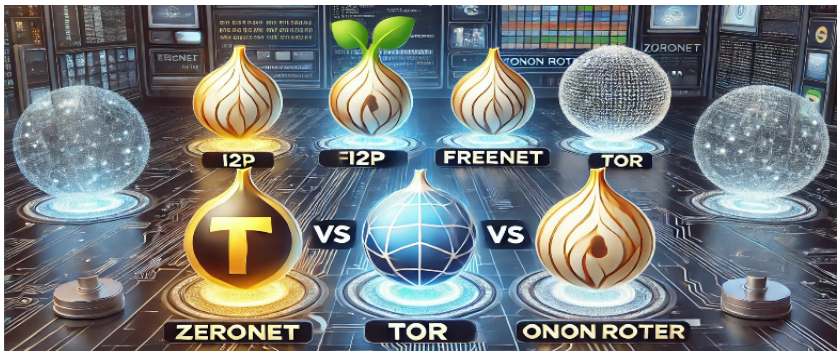
System. This system allows users to look up property assessment and tax details by entering an address.

Browsers for the Dark Web

Beyond the deep web lies the darknet, a deliberately concealed network built on top of the internet. Unlike the deep web, which is accessible with the right credentials, the darknet requires specialized tools and software such as encryption plugins or specific network protocols to access. You can’t simply enter a darknet URL into a regular web browser. Just as the internet is an internetwork connecting computers globally, darknets function as isolated networks designed for anonymity. Here are a few well-known **examples:**

- **Tor (The Onion Router):** A decentralized network of volunteer-run servers that helps users mask their location and browsing activity. Instead of making direct connections, users communicate through a series of encrypted tunnels.
- **I2P (Invisible Internet Project):** A network designed to secure private communications, preventing tracking and surveillance.
- **Freenet**: A peer-to-peer platform that allows users to share files, browse anonymous “free sites,” and engage in secure conversations.
- **Zero Net**: A decentralized network that functions similarly to darknets, using peer to peer technology.

Websites on the Tor network typically end in. onion



Tor employs onion routing, where data passes through multiple encrypted relay nodes before reaching its final destination. Each relay only decrypts one layer of encryption at a time, ensuring that no single relay knows both the sender's identity and the final recipient. Other darknets use similar encryption methods to maintain privacy and anonymity.

Who Uses the Darknet and Why?

Most discussions about the darknet focus on illegal activities. While the darknet does offer anonymity for

legitimate users—such as journalists, activists, or individuals living under oppressive regimes it also attracts criminal enterprises. Here are some of the most common illicit uses:

Drug and illegal substance trade: Darknet marketplaces facilitate anonymous transactions of drugs and controlled substances.

Counterfeiting: Fake identity documents, passports, and counterfeit money are often sold on darknet forums.

Stolen data vendors: Credit card details, Social Security numbers, and other personal data are sold for fraudulent use.

Weapons trade: Firearms and other illegal weapons are sold in darknet black markets.

Hacking services: Black-hat hackers offer their services for hire, exploit security vulnerabilities, and exchange stolen data.

Gambling: Some darknet gambling sites operate outside legal regulations.

Terrorist communication: Extremist groups may use the darknet for recruiting, information sharing, and coordination.

Murder-for-hire services: While often debated as hoaxes or law enforcement traps, some darknet sites claim to offer contract killing services.

Illegal explicit content: The darknet is unfortunately known for hosting sites involved in illicit and disturbing content. While the darknet provides valuable privacy tools for whistleblowers and political dissidents, it remains a hotspot for criminal activity. Law enforcement agencies worldwide actively monitor darknet markets and forums to track illegal operations.

.....
.....

Chapter 3

LIST OF HIDDEN LINKS

📜 ***“"The key to navigating the Dark Web isn’t curiosity, but caution and preparation."***

Every action leaves a trace—unless you know how to cover your tracks.

⚠ DARKNET: PLEASE BE CAUTIOUS!

As anywhere in life, you need to bring a healthy Part of skepticism when Employing the Darknet. Where no censorship or surveillance is possible, you'll also discover a

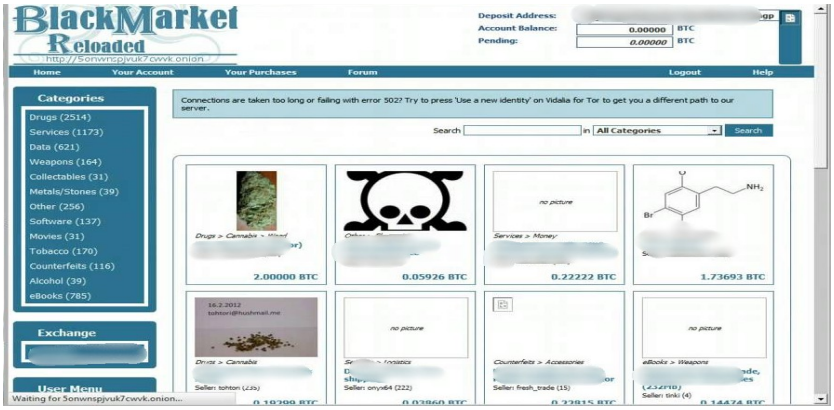
lot of shady characters. However, there aren't just trading areas for weapons or drugs!

The Most Popular Website on the Dark Web

Surprisingly, one of the most visited sites on the Dark Web is Facebook’s Onion version. This special version of Facebook enables users to access the platform anonymously, bypassing censorship in countries where it is restricted, such as China and Iran. It provides a secure way for individuals to connect with the world while maintaining privacy.

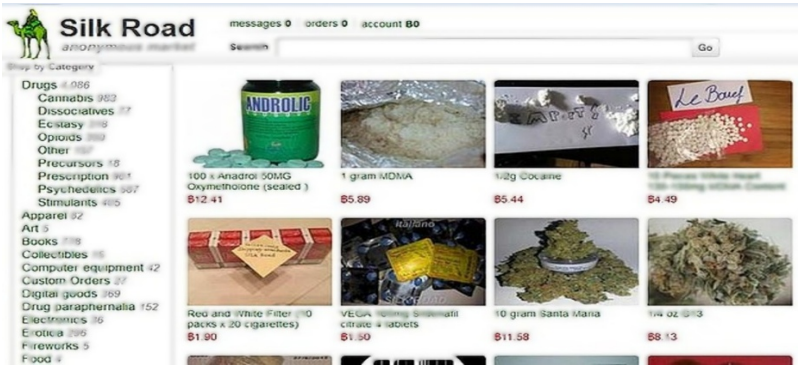
How to Find Information: Dark Web Search Engines

Because websites on the Dark Web frequently go offline, keeping track of working links can be difficult. Unlike the surface web, where Google efficiently indexes websites, the Dark Web requires specialized search engines.



Previously, Grams was the go-to search engine, often dubbed the "Google of the Dark Web." However, it has since disappeared. A newer and more reliable alternative is Torch, one of the largest Dark Web search engines, indexing thousands of .onion sites.

Several directories also help users discover sites:



Dark Web Email Services: Secure Communication

Communication on the Dark Web is often encrypted, and several email providers operate strictly within this space. One such service is Tor Box, which allows users to send and receive messages securely. However, Tor Box only functions within the Dark Web, meaning emails cannot be sent to or received from regular email providers like Gmail or Yahoo.

Dark Web vs. Surface Web: What's the Difference?

Most internet users only interact with the Surface Web—the visible part of the internet that includes search engines, social media, and news sites. Beyond that lies the Deep Web, which consists of unindexed content like medical records, private databases, and academic papers. The Dark Web is a small portion of the Deep Web that requires special tools, like Tor, to access.

Final Thoughts: Staying Safe on the Dark Web

Venturing into the Dark Web requires a cautious approach. While it offers valuable privacy tools and resources, it is also home to potential risks, including scams, phishing sites, and malicious software. To stay safe:

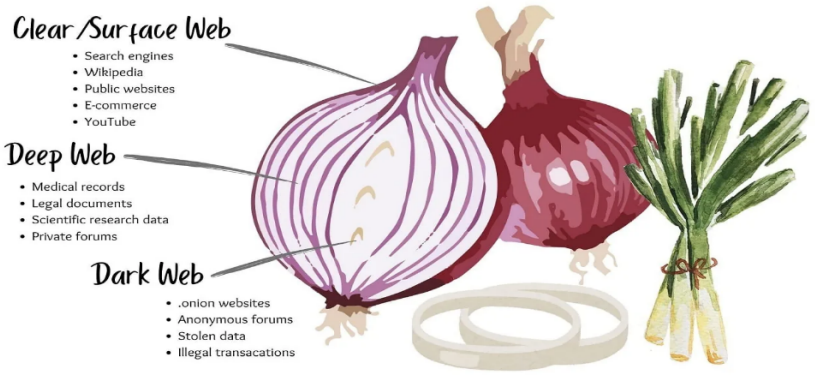
✅ Always use Tor with a VPN for additional security.

✅ Never reveal personal information.

✅ Avoid downloading unknown files.

✅ Use trusted Dark Web directories and search engines.

✅ Be mindful of potential scams and fake services.

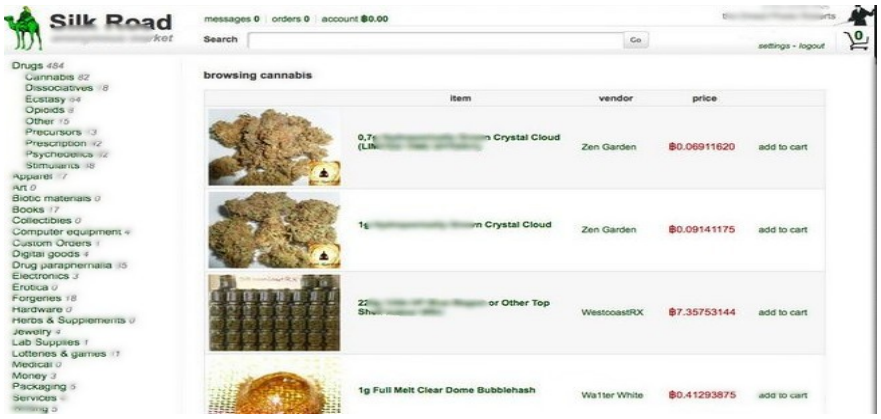


By following these best practices, users can explore the Dark Web while minimizing risks. Whether you're seeking privacy, researching hidden information, or simply curious about this underground network, knowledge and caution are your best allies.

Infamous Cases of this Dark Web

When most people think of the dark web, a few notable examples come to mind—often those that have made headlines for their illicit activities. Many of these websites or networks operate in legally gray or outright illegal areas. However, not all dark web marketplaces are necessarily unlawful. One of the most well-known examples was the Silk Road marketplace. Launched in 2011, Silk Road became infamous for facilitating the trade of illegal goods, including narcotics, counterfeit documents, and firearms. It was among the first dark net markets to operate with Bitcoin,

taking advantage of its anonymity for transactions. However, the site was seized and shut down by the FBI in 2013, and its founder, Ross Ulbricht, was sentenced to life in prison.

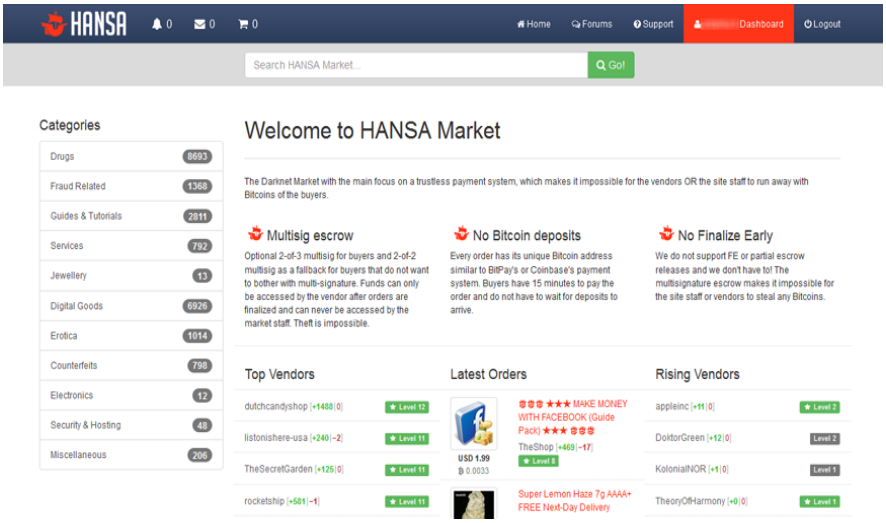


Alpha Bay (2014–2017)

One of the largest dark web marketplaces after Silk Road’s demise, Alpha Bay facilitated the sale of illicit drugs, hacking tools, and stolen financial information. It was shut down by the U.S. Department of Justice in 2017, leading to the arrest of its founder, Alexandre Cazes, who was later found dead in his prison cell.

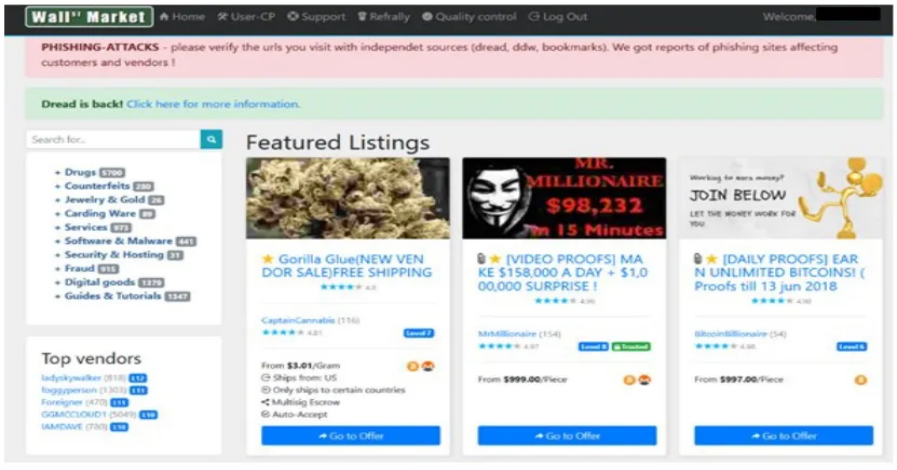
Hansa Market (2015–2017)

This marketplace gained popularity after Alpha Bay’s shutdown, but in a dramatic turn of events, it was secretly taken over by Dutch law enforcement in 2017. The authorities operated the site for a month, gathering user data before closing it down.



Wall Street Market (2016–2019)

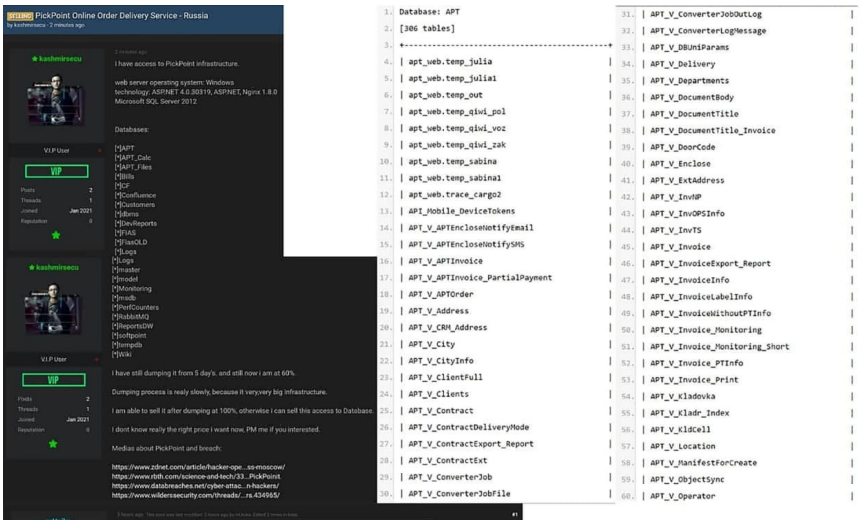
Another significant dark web marketplace, it facilitated illegal trade before being seized by Europol in 2019. Its administrators were arrested, and millions of dollars in cryptocurrency were confiscated.



Dark Market (2021)

This was one of the largest illegal markets on the dark web, with nearly 500,000 users. It was taken down by German authorities in a coordinated operation involving multiple countries.

While these marketplaces are often linked to illegal activities, the dark web itself is not entirely unlawful. It is also used by journalists, activists, and whistleblowers to communicate securely. For instance, media organizations like The New York Times and



Reasons to Use or Avoid the Dark Web

Besides prohibited purchases and sales, there are valid reasons one may Be interested in utilizing the dark web. People within closed societies and confronting intense censorship can use the dark web to communicate with other people beyond the society. Even people within open societies might have some interest in utilizing the dark web,

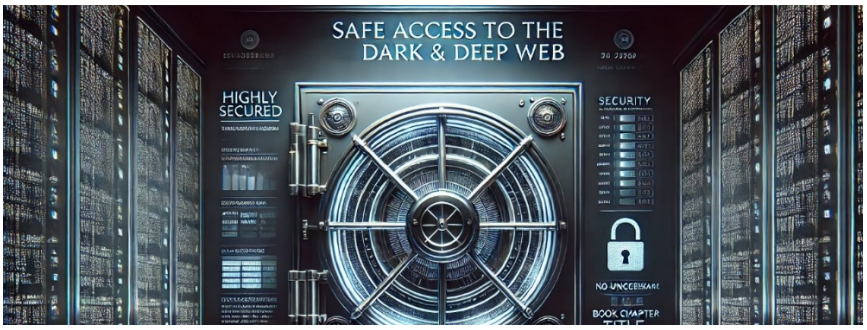
especially as concerns regarding government snooping and data collection continue to rise globally. It is not tough to surmise why this could be the situation: the dark web offers a degree of individuality safety the surface internet doesn't. Criminals seeking to secure their identities so as to prevent detection and capture have been attracted to the facet of the dark web. Because of this, it is unsurprising that several noteworthy hacks and information breaches are linked with the dark web in some manner or another.

In 2015, as an Example, a trove of consumer info was stolen out of Ashley Madison, a site purporting to provide spouses a way of cheating on their spouses. The stolen information showed on the dark web, where it was later recovered and shared with the general public. In 2016, then-U.S. Attorney General Loretta Lynch cautioned that gun sales happening over the dark internet were becoming more prevalent, as it enabled buyers and sellers to prevent regulations. Illegal

pornography is another relatively common occurrence on the dim web.

Chapter 4

SAFE ACCESS TO DARK WEB



📜**“"*Anonymity is a double-edged sword—protect yourself before stepping into the unseen corners of the internet.*"**

Knowing the risks before you enter can make the difference between safety and exposure.

The internet you browse daily represents only a small fraction of the vast World Wide Web. According to estimates, the web contains nearly 500 times more content than what Google indexes in its search results. The part of the internet

that search engines like Google can access is called the "surface web," while the non-searchable portion is known as the "deep web" or "invisible web."

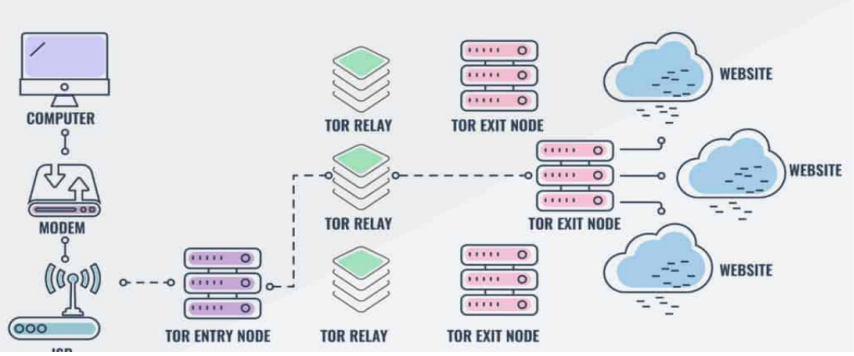
Understanding the Deep Web

Much of the deep web remains hidden simply because most users do not require access to it. Many of its contents are stored in databases that Google does not index or is restricted from crawling. Examples include academic journals, court records, private social media profiles, documents stored in cloud services, and content within mobile applications. While these resources exist online, they are not automatically accessible through search engines.

⚠Caution: Your ISP Can Detect Tor Usage

A significant part of this guide focuses on anonymity networks like Tor, which allow users to access the dark web. However, internet service providers (ISPs) can detect when someone is using Tor, as Tor node IP addresses are public.

To maintain privacy, users can utilize a VPN or Tor Bridges —alternative nodes that are not publicly listed. For U.S.-based Tor users, using a VPN is often recommended, as it provides better speed and reliability. Due to recent changes in U.S. laws, ISPs can collect and sell user data, including browsing history.



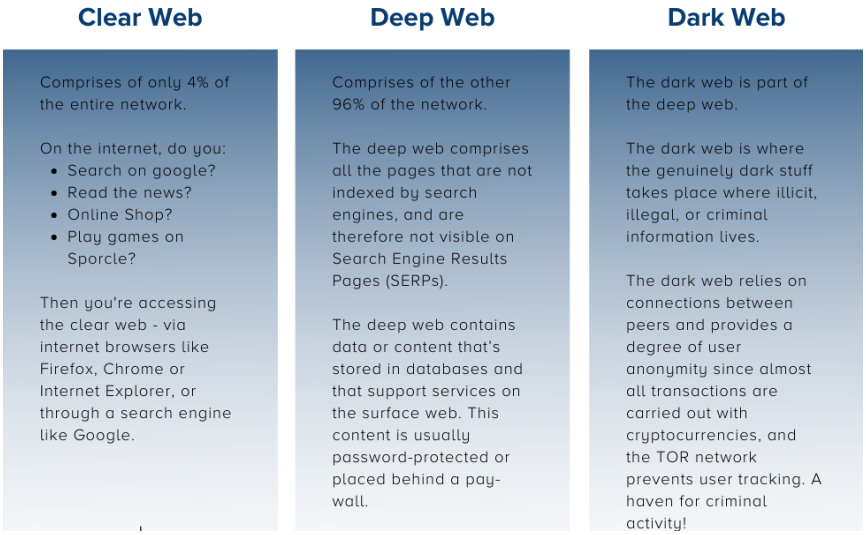
Deep Web vs. Dark Web: the deep web is often confused with the dark web, also referred to as the darknet or black web. In simple terms, the deep web consists of all online content that is not indexed by search engines. Unlike the dark web, it does not require specialized tools for access—users just need to know where to look.

WWW Virtual Library: The first web index, functioning more as a directory than a search engine.

Surf wax: Indexes RSS feeds (though its functionality may be limited now).

Ice Rocket: Searches blogs and Twitter for deep web content.

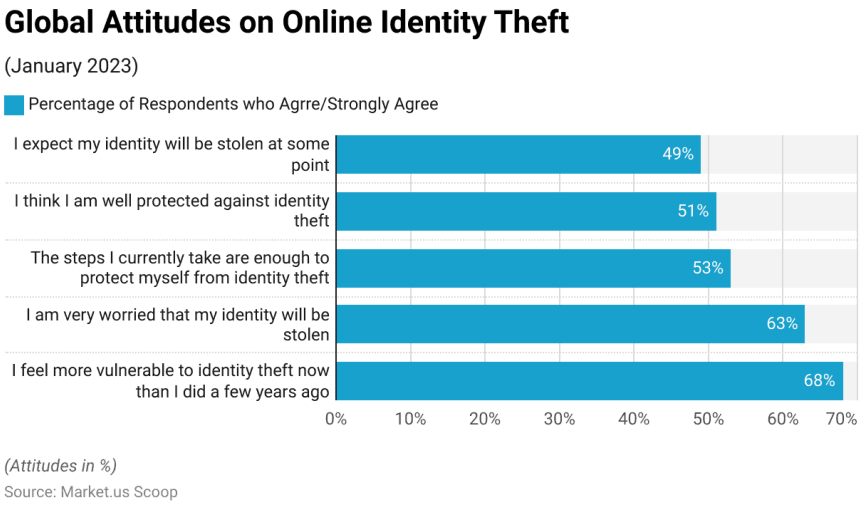
For example, legal records can be found in public court archives, while academic papers are available in research databases. Users can also refine searches using specific file types, such as PDFs or Excel spreadsheets, by using operators like "filetype: PDF" in search queries.



The Dark Web: Anonymity and Risks

The dark web is a small subsection of the deep web that is intentionally hidden. Unlike the deep web, dark web content requires specialized tools—such as the Tor browser—to access. The dark web is often associated with illegal activities, such as marketplaces for drugs, weapons, and stolen financial information. However, it is also used for legitimate purposes, such as private forums, anonymous communication, and secure whistle blowing. One of the defining features of the dark web is its emphasis on anonymity. Users can operate without being tracked by

corporations or governments, provided they take proper security measures. Journalists, activists, and whistleblowers —including Edward Snowden—have used the dark web to share sensitive information. The Ashley Madison data leak, for example, was first posted on a site accessible only through Tor.



How to Safely Access the Dark Web

The dark web is decentralized, much like the surface web, with servers distributed worldwide. The safest way to access it is through the Tor network (The Onion Router). Dark web addresses typically end in “. onion" instead of common domains like ".com" or ".org", indicating that they are only accessible via Tor.

Steps to Access the Dark Web:

Download and Install the Tor Browser – The most secure way to browse the dark web is through the Tor Browser, which is

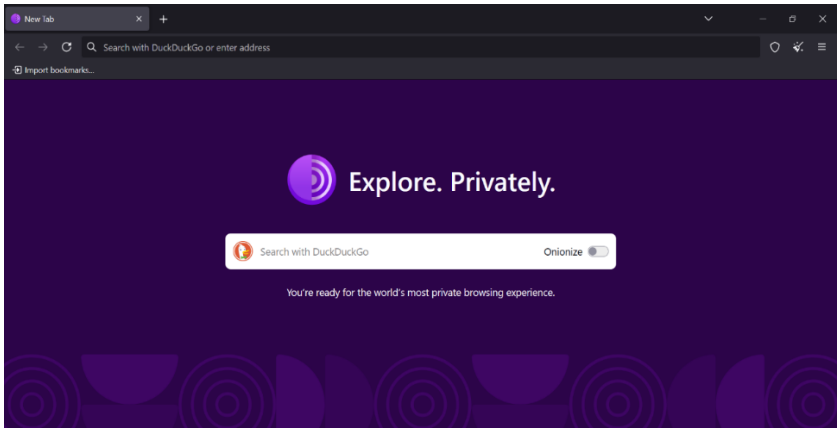
based on Firefox and routes traffic through multiple encrypted relays.

Ensure You Download from the Official Source

To avoid malware, always download the Tor Browser from its official website.

Avoid Third-Party Tor Browsers

Officially, the Tor Browser is available for Windows, Mac, and Linux. Using third-party Tor-based browsers on other platforms may pose security risks.



By following these precautions, users can navigate the dark web securely while minimizing the risks associated with online anonymity tools.

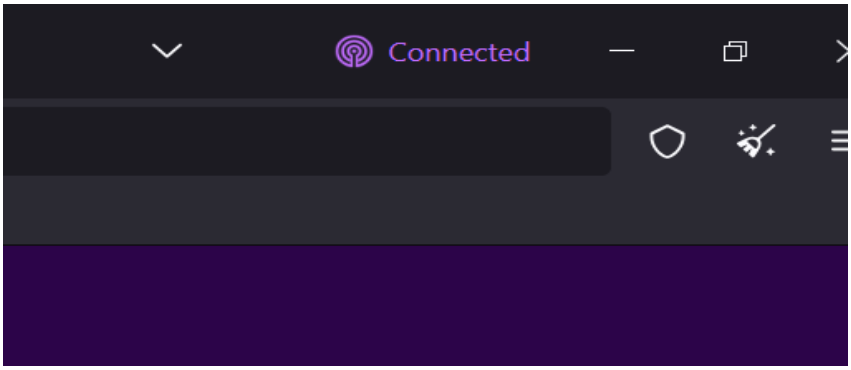
Access dark net on Android using Tor Browser (UPDATE)

The official Tor Browser is currently available on Android. You can get it out of The Play Store or the Tor downloads

webpage. As of writing, Tor Browser for Android is still in alpha, and also requires you set up Orbot for a prerequisite.

Navigating the dark Web

Now you Can safely navigate dark net sites and concealed wikis, but if you intend to do anything longer than that, you will want to take several steps. Meaning setting up encrypted email using a brand-new email address, with a pseudonym, establishing an anonymous bitcoin wallet, disabling JavaScript from Tor Browser, exploring vendors, and much more.



Finding. onion sites is your first challenge, as they won’t appear in Google search results. You can't simply Google "Silk Road" and expect to land on the dark web. However, some dark web search engines index. onion websites, including Onion. City, Onion.to, and Not Evil. If you're searching for specific goods, especially medications and narcotics, you can use Grams.

Reddit can also be a valuable resource for navigating the dark web. Subreddits like /r/deep web, /r/onions, and /r/Tor can help. Additionally, hidden wiki directories can assist in narrowing your search.

Anonymity and security are crucial when browsing the dark web. While your ISP and the authorities may not be able to see your activities on the Tor network, they can detect that you're using Tor, which may raise suspicions. In fact, a recent U.S. Supreme Court ruling stated that merely using Tor could be considered probable cause for law enforcement to investigate any computer worldwide. Another critical precaution is ensuring that your .onion URLs are accurate. These URLs typically consist of a random series of letters and numbers. Since HTTPS is rarely used on the dark web, SSL certificates cannot verify site legitimacy. Always confirm a URL from at least three different sources before using a dark web site. Once verified, store it in an encrypted note—Tor browser does not cache URLs. Otherwise, you risk falling victim to scams like fake Bitcoin mixers.

For additional security, using a VPN is highly recommended.

VPN Over Tor vs. Tor Over VPN

A VPN encrypts all internet traffic traveling to and from your device and routes it through a server of your choice. When combined with Tor, it enhances security and anonymity. While similar in purpose, Tor prioritizes anonymity, whereas

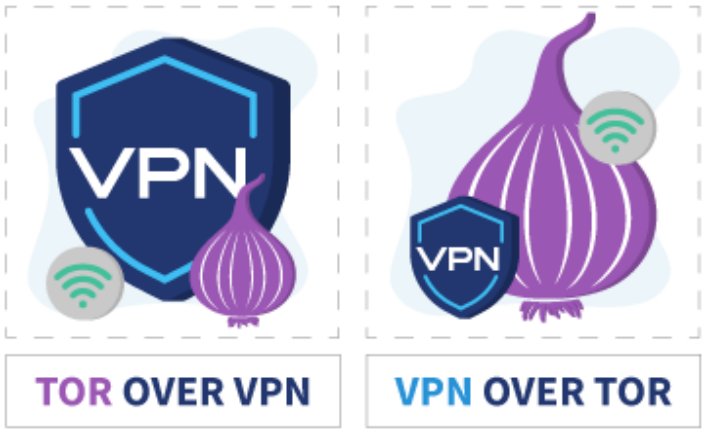
a VPN focuses on privacy. Combining both reduces risk, but the order in which they are used makes a significant difference.

Tor Over VPN

If you connect to a VPN first and then use the Tor browser, you are employing Tor over VPN, the most common method. In this setup:

Your ISP only sees encrypted VPN traffic and won’t know you're using Tor. You can access. onion sites normally. However, this method requires trust in your VPN provider, which can see that you're using Tor and may keep metadata logs, even if it cannot see the contents of your Tor traffic. Choosing a no-log VPN is crucial. Some VPNs, such as NordVPN, offer built-in Tor over VPN functionality, allowing you to access Tor without using the Tor browser. However, other browsers may still leak identifying data.

Tor over VPN does not protect users from malicious Tor exit nodes. Since Tor nodes are run by volunteers, some may attempt to intercept data.



VPN Over Tor

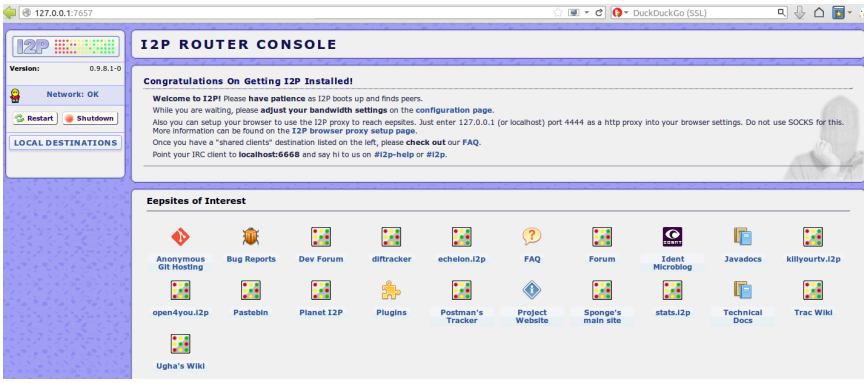
Less common but recommended by the official Tor Project, VPN over Tor works differently:

1. Internet traffic is first routed through Tor, then through the VPN.
2. The VPN provider does not see your real IP address.
3. The VPN protects you from malicious Tor exit nodes.
4. Only a few VPN providers, such as AirVPN and BolehVPN, support VPN over Tor. However, they are not known for high speeds.

Tor over VPN is better for accessing. onion sites, while VPN over Tor is ideal for avoiding malicious Tor exit nodes. Some argue VPN over Tor is more secure as it preserves anonymity throughout the process, assuming the VPN is paid for anonymously. While the Tor Project advises against VPN over Tor, both methods are safer than using Tor alone.

I2P

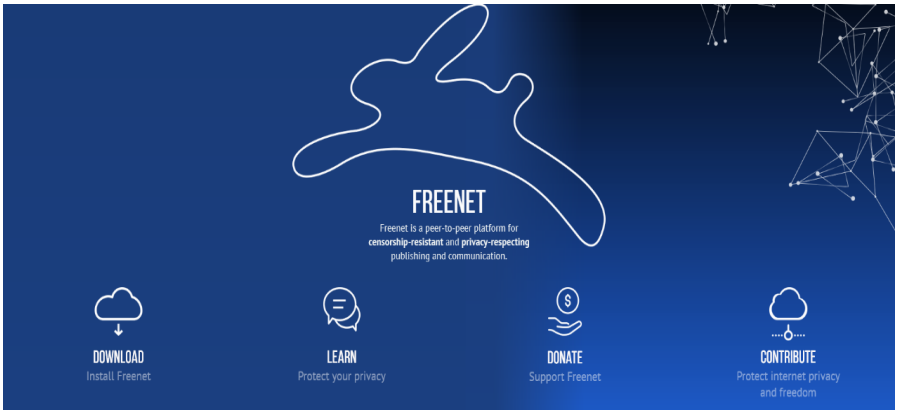
I2P (Invisible Internet Project) is an alternative anonymous network to Tor. Unlike Tor, I2P cannot access the regular internet; it can only reach hidden services within the I2P network. It does not support. onion sites, as it operates on a separate network, using "respites" instead.



While less popular and more complex to set up, I2P has some advantages over Tor: It is faster and more reliable due to its advanced peer-to-peer routing system. It does not rely on a centralized directory for routing information.

Freenet

Like I2P, Freenet is a decentralized, peer-to-peer network that does not allow access to the standard internet. Instead, users can only access content uploaded to Freenet’s distributed data store. Unlike I2P and Tor, hosting content does not require a dedicated server. Once uploaded, content remains on Freenet as long as it remains popular.



Freenet offers two connection modes:

Darknet mode: Users connect only with trusted peers, creating private, anonymous networks.

Open net mode: Users automatically connect to random peers and use a few dedicated servers for routing.

Freenet is relatively easy to use. After installation, it runs through a browser interface. However, for security reasons, it is recommended to use a separate browser from your usual one to maintain anonymity.

Search Engines and the Deep Web

Google and Bing dominate the search engine market, with Google holding about 92% and Bing around 3%. They automatically index vast amounts of data, but they do not cover everything. Many websites deliberately hide from search engines, making up what is known as the Deep Web.

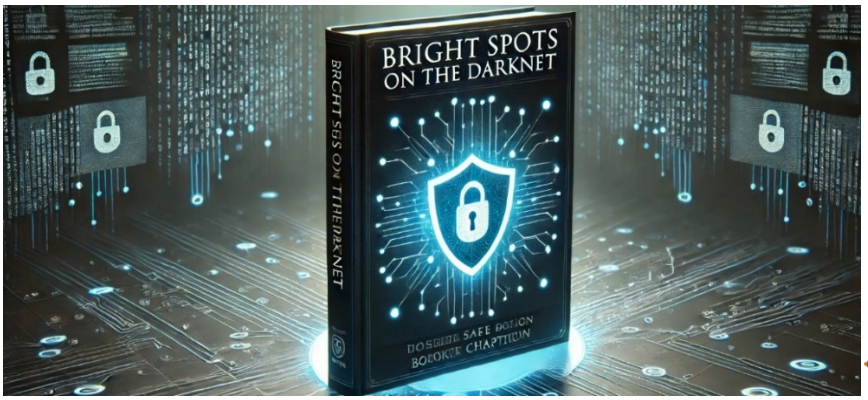
Is the Darknet Illegal?

No, the darknet itself is not illegal. It is simply an uncensored, unregulated part of the internet. It is used by activists, journalists, and researchers, but also by criminals. Its anonymity makes it a double-edged sword.

The darknet remains one of the last bastions of free speech, allowing people to communicate without fear of surveillance. However, it also provides a platform for illegal markets, hacking forums, and illicit content. For those exploring the dark web, knowledge, caution, and security measures are essential to staying safe.

Chapter 5

BRIGHT SPOTS ON DARKNET



📜***""Not everything in the shadows is sinister—sometimes, the brightest lights shine where least expected."***

The Darknet isn’t just a place for criminals—whistleblowers, researchers, and activists rely on it too.

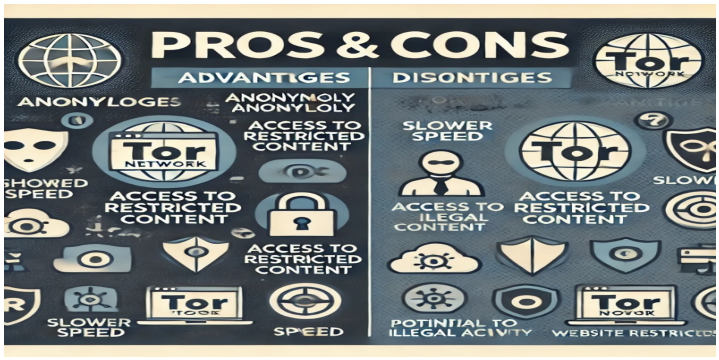
The darknet is not just a hub for illegal or questionable content. While it undeniably hosts criminal marketplaces, malware forums, and other underground activities, it also contains a few legitimate websites and communities. To be clear, the darknet remains a high-risk and unregulated space. You shouldn't simply download a Tor browser and start exploring without understanding the risks.

According to TechRepublic, the darknet hosts an estimated 10,000 to 100,000 websites, while the Tor network has roughly two million active users worldwide. Some of these users engage in illicit activities, but many simply seek

anonymity while browsing the surface web or contributing to legitimate, valuable darknet communities.

10 Bright Spots on the Darknet

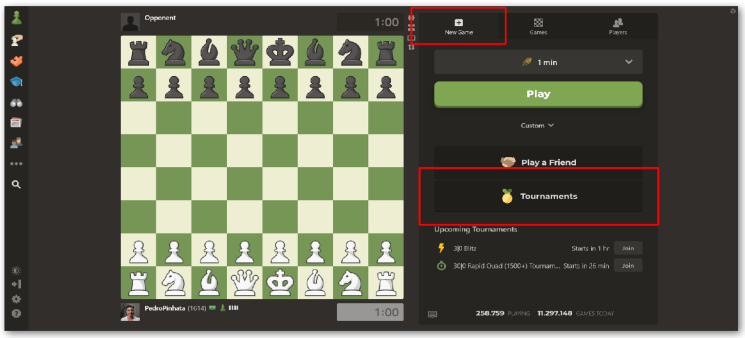
The Darknet isn’t just a hub for cybercrime there’s also a hidden world of useful and even fascinating websites. When most people hear "darknet," they think of illegal activities—black markets, hacking forums, and disturbing content lurking in the shadows of the internet. And yes, those things do exist. But the darknet is not all doom and gloom. Surprisingly, there are many legitimate, informative, and even fun places tucked away in the depths of Tor. Whether it’s anonymous gaming, uncensored journalism, or academic research, this mysterious corner of the internet has some bright spots worth knowing about.



1. The Chess – Play Anonymous Chess Matches

Imagine a place where you can play chess against strangers without usernames, without chat, and completely anonymous. That’s exactly what The Chess offers. You create

a temporary account and can play unlimited chess matches. There’s a small forum where users discuss strategies. However, the biggest downside is that the website looks like it's straight out of Windows 95 functional, but very outdated.



2. Academic Research – Free Access to Knowledge

Education should be free, right? The darknet has some controversial but useful resources for academic research. Sci-Hub is a well-known darknet tool that provides access to thousands of academic papers. However, it's legally questionable. A more ethical alternative is the American Journal of Freestanding Research Psychology (AJFRP)—the first-ever open-access academic journal hosted on the darknet. Unlike Sci-Hub, this is completely legal, as authors submit their own work voluntarily.

3. ProPublica – Uncensored Journalism

In countries where the government censored news, accessing the truth can be dangerous. That's where ProPublica's darknet version comes in. ProPublica is a Pulitzer Prize-winning investigative journalism platform. People in censored regions can read independent news safely, without leaving digital traces. Unlike regular news sites, ProPublica doesn't track your data.

"*We don't want anybody to know that you came to us or what you read.*" **Mike Tiga's**

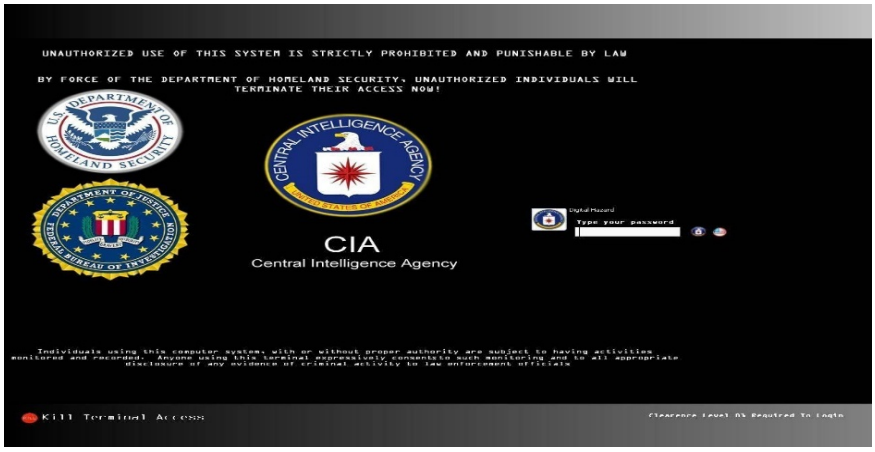
4. Secure Drop – Whistleblowers' Safe Haven

Ever wondered how whistleblowers safely leak information to journalists? Secure Drop is the answer. It's widely used by major outlets like The Washington Post, The New Yorker, Vice Media, and Forbes. Secure Drop doesn't record IP addresses or store browser data, ensuring maximum security for those who submit confidential information. Even the U.S.

government is testing it for anonymous security vulnerability reports.

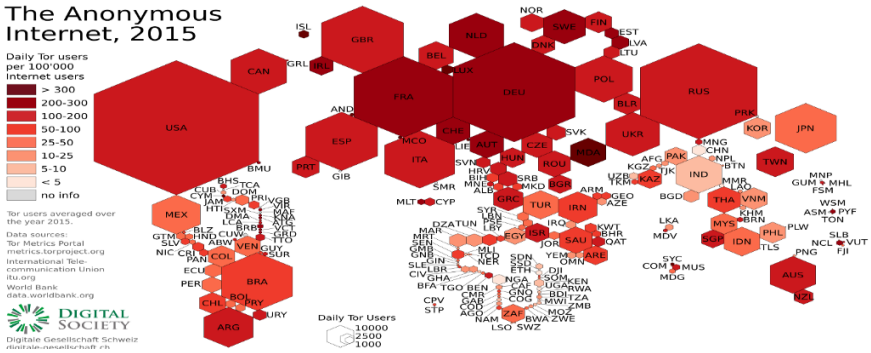
5. The CIA’s Hidden Website

Yes, even the CIA has a darknet website. It’s a simple contact form where people can anonymously submit information. The agency guarantees to "carefully safeguard all information you provide, including your identity." While it's not a full-fledged intelligence platform, it’s one of the more surprising government presences on the darknet.



6. Tor Metrics – Who Actually Uses Tor?

Think the darknet is only for criminals? 60% of Tor usage is completely legal. Tor Metrics is a public data website that tracks how many people use Tor worldwide and for what purposes. Political censorship remains one of the main reasons people turn to Tor, while many journalists, researchers, and everyday users rely on it for online privacy.



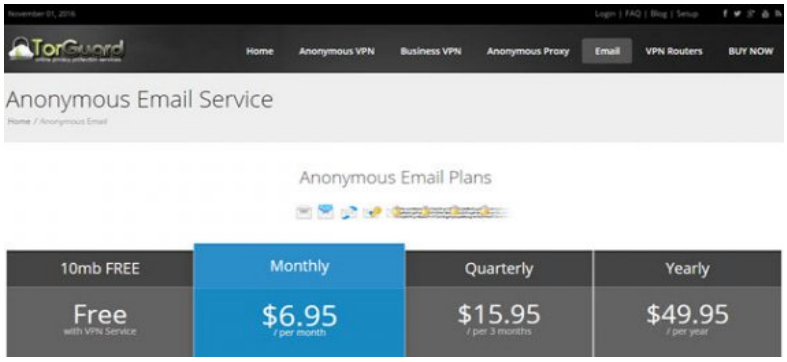
7. IIT Tunnels – Real-Life Urban Exploration

Deep under Illinois Institute of Technology (IIT) lies a mysterious network of abandoned underground tunnels. A darknet user spent months exploring these tunnels and published photos and maps online. No one knows exactly why they were built—some say they were for steam pipes, while others believe they were secret access points for the university. This discovery has sparked both fascination and conspiracy theories.

8. Anonymous Email Services – Privacy First

In a world where Google, Yahoo, and Outlook track everything, darknet email providers offer a privacy-focused

alternative. One of the most well-known is Proton Mail, developed by scientists at MIT and CERN. Proton Mail offers end-to-end encryption, and unlike mainstream email providers, it doesn't require any personal data to create an account.



9. Ad-Free Search – No Tracking, No Ads

Hate online ads? DuckDuckGo is a darknet-friendly search engine that:

1. Doesn't track users
2. Doesn't store search history
3. Has zero ads

Unlike Google, DuckDuckGo won't sell your data. It's not just for the darknet—you can use it on the surface web too.

10. Tor Kittenz – The Cutest Part of the Darknet

Believe it or not, someone made a Tor-only website that was just a gallery of cat pictures. It had a retro 90s-style design, and while it no longer exists, it was one of the few purely wholesome darknet sites, proving that not everything in the hidden corners of the web is sinister.

Final Thoughts: The Darknet Isn’t Just Crime & Chaos

Yes, there are dangerous places on the darknet. But, as we've seen, there are also positive and useful parts—

educational tools, secure communication, and even simple fun like playing chess or sharing cat photos. Curiosity is good, but safety comes first. If you ever decide to explore, make sure to use proper security measures and stick to trusted sites.

⚠ IMPORTANT NOTE:

Never attempt to access. onion websites through a regular web browser. If you choose to explore the darknet, do so cautiously, using appropriate security measures.

Chapter 6

UNVEILING HIDDEN INTERNET

📜**“"*Tor isn’t just a tool—it’s a gateway to anonymity, for better or worse.*"**

———————

Whether you seek privacy or secrecy, understanding Tor is the first step

The World Wide Web, at its core, is a network of computers communicating with each other. Computer A requests information from Computer B, and Computer B sends back the data. This data can be a webpage, an advertisement, a calculation almost anything.

Each computer involved in this exchange has a unique identifier known as an **IP address (Internet Protocol)**. These addresses look something like this: 29.75.148.222. Since IP addresses are difficult to remember, they are often replaced with domain names. For example, when you type "**facebook.com**" your Internet Service Provider (ISP)

translates that domain into the corresponding IP address of Facebook's server. Facebook then responds by delivering the requested data to your computer. This method of communication applies to all areas of the internet, including the deep web and the dark web. The difference between these and the regular web lies in how easily content can be found.

The Deep Web vs. The Surface Web

When you search Google for Facebook, CapitalOne, or TSN, you receive indexed results—these are examples of the surface web. Anything that appears in search engine results is part of this indexed web. However, not all content is searchable. **For example**, private WhatsApp conversations, personal emails, banking portals, or even classified ads on certain websites are inaccessible via traditional search engines. This unsearchable portion of the internet is what we call the deep web. The deep web also contains a vast amount of data that is constantly generated by machines—such as system logs, health monitoring reports, and server communications. Most of this information is uninteresting to the average user. In fact, the searchable surface web makes up only around 10% of the entire internet, while the deep web accounts for the remaining 90%.

The Deep Web vs. The Dark Web

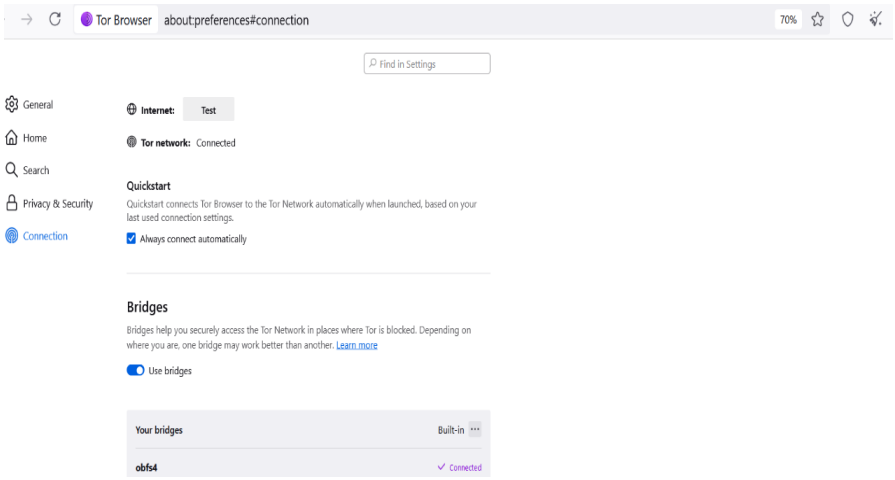
People often use the terms "deep web" and "dark web" interchangeably, but they are quite different. The dark web is a small part of the deep web, much like a hidden layer beneath the already concealed deep web. Unlike the general deep web, which includes unsearchable but normal content, the dark web is intentionally designed for anonymity and requires specialized tools to access. Because the dark web allows users to hide their identities, it has gained a reputation as a hub for illegal activities. However, its origins are not as sinister as one might think. Before the internet became mainstream, early online users engaged in anonymous discussions via **Internet Relay Chats (IRC).** Some of today's criminal activities on the dark web can be traced back to those communities. That being said, not everything on the dark web is illegal. Many people use it for legitimate reasons, such as whistleblowers who need to protect their identities or individuals living in countries where internet censorship restricts access to information. Unlike the deep web, which can be accessed if you have a direct link, the dark web requires a specialized browser. Even if a user finds a link to a dark web site, they cannot access it through traditional browsers like **Chrome or Firefox.**

It's important to note that while the iceberg metaphor is commonly used to describe the internet where the surface web is the tip, the deep web lies below, and the dark web is

even deeper—this is not entirely accurate. In reality, these different sections exist alongside each other in the same space, hidden in plain sight rather than existing in separate digital compartments.

Accessing the Dark Web: The Role of Tor

The dark web's most infamous marketplace was Silk Road, which was shut down by the FBI in November 2014. What made Silk Road a "dark" website? To access dark web sites, users must use a specialized browser called Tor. Tor looks like any other browser, but it provides anonymity through a method known as onion routing.



The name "Tor" itself stands for "The Onion Router" Onion routing works by bouncing a user’s internet traffic through multiple computers, known as nodes or relays, before reaching the final destination. Any computer running Tor

software can act as a node. By passing through multiple layers of encryption, it becomes nearly impossible to trace the original source of the request. However, this process makes browsing extremely slow. While Tor users can visit regular websites just like they would on Chrome or Firefox, dark web sites have unique domain extensions that end in “. onion" instead of ".com" These sites can only be accessed through the Tor browser.

The Origins of Tor: Who Created It?

Contrary to popular belief, Tor was not developed by hackers or cybercriminals. It was actually created by the U.S. government. The concept of onion routing was first funded by the U.S. Office of Naval Research in 1995 and later improved with support from the Defense Advanced Research Projects Agency (DARPA) in 1997. The technology was eventually released to the public in 2002.

Can Tor Be Hacked? Is Anonymity Truly Secure?

Tor itself is highly secure, and hacking the algorithm is considered nearly impossible. However, no system is entirely foolproof. If law enforcement or cybercriminals want to track someone using Tor, they don’t attack the technology itself they target human error.

World War II, the Germans' Enigma machine

For example, during World War II, the Germans' Enigma machine was cracked not by brute force but through an understanding of human patterns and behaviors. There are also vulnerabilities in the way Tor operates. While the browser protects users from being traced directly, it does not prevent them from accidentally downloading malware that could reveal their identity. Additionally, Tor's exit nodes —where encrypted traffic leaves the network—can be monitored, potentially exposing users' activity.

Why Is Information About the Deep Web and Dark Web Important?

Since the deep web and dark web offer anonymity, they have become hotspots for illegal activities. However, these hidden areas also provide valuable intelligence for cybersecurity experts, law enforcement, and corporations. For example, the deep web contains unindexed forums where individuals may incite hate speech, coordinate threats, or discuss illegal activities like shoplifting and drug use. Similarly, paste sites like Pastebin are often used to share leaked data. The dark web takes illegal activity to another level. While many sites

are scams, others serve as marketplaces for drugs, stolen data, illegal services, and worse.

7 Ways that the Hidden World of the Darknet Is Evolving

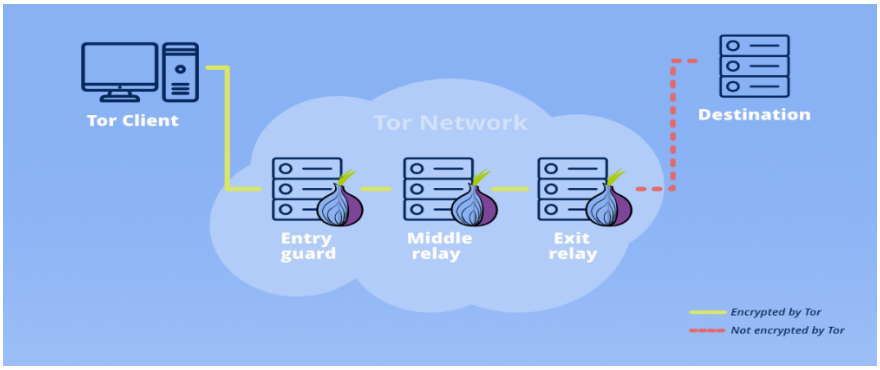
The darknet isn't as hidden as it once was. What was once a secretive part of the internet is now becoming more accessible. Today, anyone with basic technical skills can download a Tor browser and start exploring, often using cryptocurrency for anonymity. But with greater accessibility comes greater risks. Cybercriminals use the darknet to sell narcotics, stolen data, and illegal services. Law enforcement agencies have intensified their crackdown. Ross Ulbricht, the founder of the infamous Silk Road marketplace, is now serving two life sentences plus 40 years for drug trafficking and money laundering. Even within the darknet, things are changing.

1. The Battle Isn’t Over

Despite its increasing visibility, the darknet remains a battleground. Beyond well-known marketplaces and widely reported cases, the real danger lies in hard-to-reach corners of the internet—hidden forums, encrypted chatrooms, and secret data leaks. For businesses, this presents a growing cybersecurity threat. Studies indicate that hidden risks are expanding rapidly, with many organizations unaware of how their sensitive data is being circulated within these secret networks.

2. The Darknet Extends Beyond Tor

Many people mistakenly believe that the darknet is limited to sites accessible via the Tor browser. However, the darknet extends beyond. onion websites. "The darknet is any online space that is not readily available to the public," explains Andrei Barysevich of Recorded Future. Some darknet hubs predate Tor and continue to function using alternative protocols like I2P, GNU net, and Riffle.



3. Enterprise Threats Are Increasing

The darknet isn't just for illicit drug sales. It also harbors cybercriminals selling tools and services that specifically target corporations. A study by Bromium found a 20% rise in darknet listings that pose threats to businesses between 2016 and 2019. These include:

1. Targeted malware
2. Corporate-specific DDoS attack services
3. Stolen corporate data
4. Brand-spoofing phishing kits

Many of these sellers are highly secretive 70% of vendors only communicate through private channels.

4. Cybercrime Trends Mirror Enterprise Threats

Darknet activity often reflects trends in mainstream cybersecurity threats. One growing concern is whaling attacks, where high-profile executives are targeted through social engineering. A 2019 IBM X-Force report revealed that

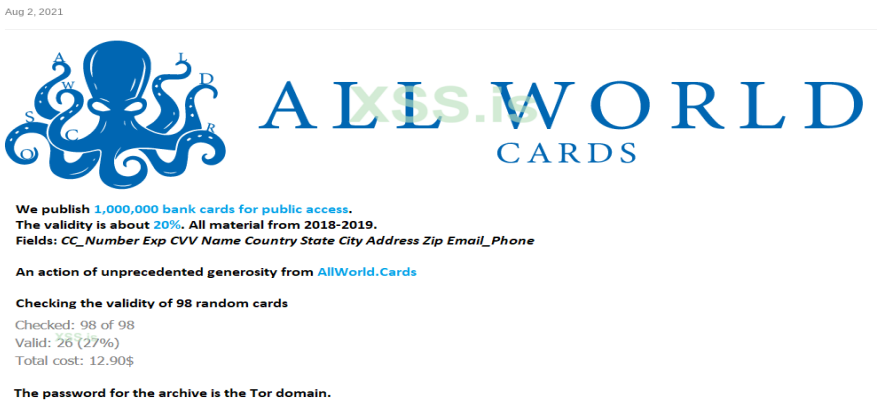
13% of all cyberattacks involved business email compromise (BEC) or whaling.

5. Stolen Digital Identities Are Sold in Bulk

In 2019, cybercriminals began selling entire digital identities. These include:

1. Banking and social media login credentials
2. Web cookies and browser fingerprints
3. HTML5 canvas fingerprints

Prices range from $5 to $200 per identity, making it easier than ever for cybercriminals to impersonate individuals.



6. Corporate Network Access Is for Sale

Bromism researchers discovered that many cybercriminals offer backdoor access to corporate systems, with at least

60% of vendors selling unauthorized access to multiple high-profile networks.

7. Intellectual Property Is at Risk

When Bromism researchers asked a darknet seller about accessing three major corporations, they were offered:

1. CEO account access
2. Server data extraction services
3. Custom hacking tools
4. Prices ranged from $1,000 to $15,000 per breach.

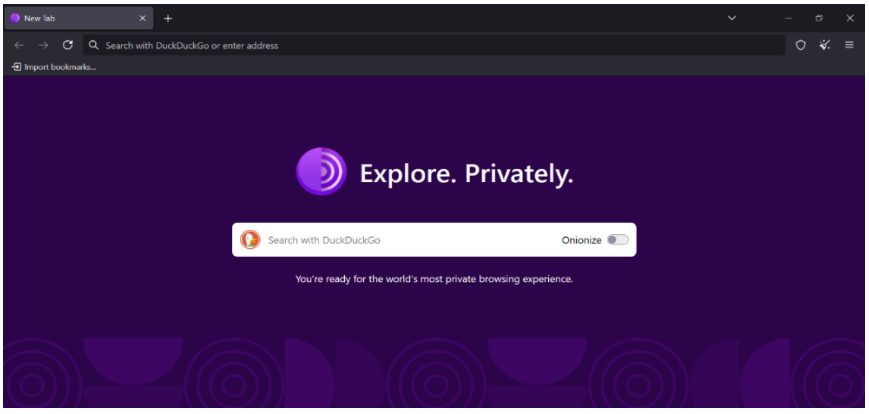
Conclusion

The surface web is what most people use daily and is indexed by search engines. The deep web is much larger and includes unindexed but mostly harmless content. The dark web is a small but significant part of the deep web, designed for anonymity and often associated with illegal activities.

While the dark web is known for its criminal markets, it is also used for privacy and free speech in countries with censorship. Information from the dark web is crucial for cybersecurity, law enforcement, and other organizations aiming to prevent illegal activity. Understanding these distinctions helps separate fact from media exaggeration. Not everything on the dark web is criminal, but it remains a place where security risks and anonymity collide.

Chapter 7

HOW TO USE TOR



📜“"***Privacy is a right, but only those who master the tools of anonymity can truly claim it.***"

———————

Knowing how to configure Tor properly is the difference between being hidden and being exposed.

Recently, Boing Boing shared an article about some librarians in Massachusetts who have begun using Tor software on all public computers to anonymize browsing activity for their users. The librarians are doing this as a stand against unchecked government surveillance and companies that track users online to create targeted marketing profiles.

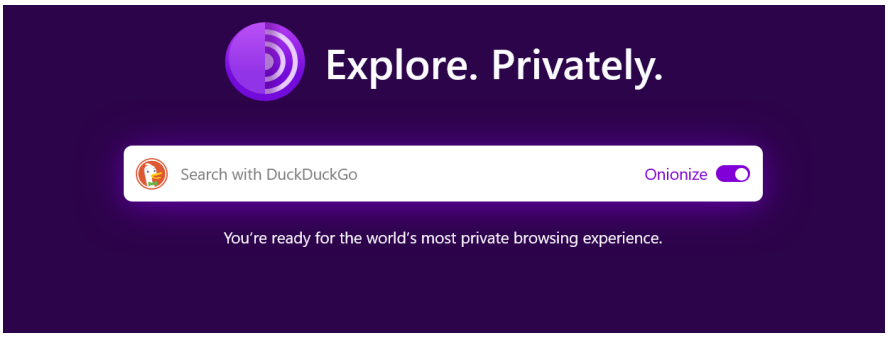
It's an intriguing initiative and a solid stance for user privacy. Fortunately, you don’t have to visit a library to use Tor. Connecting to the Tor network from your own computer is quick and easy, thanks to the Tor Project's user-friendly Tor Browser.

What is Tor?

Tor is a global network operated by volunteers. Each volunteer runs a "relay," which is simply a computer that runs software enabling users to connect to the internet through the Tor network.

Before reaching the public internet, Tor Browser connects to several different relays, ensuring your activity is

anonymized along the way, making it nearly impossible to trace your location and identity. Although Tor has gained a reputation for being used to purchase illicit products online, the software has many legitimate applications. Activists hiding their location from oppressive governments and journalists communicating with anonymous sources are just two examples.



If, like the librarians in Massachusetts, you don't have any nefarious intentions, Tor is still an excellent tool to keep your browsing private from your Internet Service Provider (ISP), advertisers, and passive government data collection. However, if agencies like the NSA decided to actively target your browsing, that's a different story altogether.

Getting Started

The easiest way to use Tor is by downloading the Tor Browser. This is a modified version of Firefox, combined with other software that connects you to the Tor network.

Some users prefer verifying the installer to ensure they've downloaded the correct, untampered version. If you're just looking to keep your browsing private, you can use Chrome's Incognito Mode, Firefox's Private Browsing, or Microsoft Edge's InPrivate mode. While these prevent others from seeing your browsing history, they don't stop your ISP from tracking the sites you visit. If you want to browse the web completely anonymously, Tor Browser is what you need.

Using Tor Browser: Step-by-Step

Install and Configure Tor Browser

Begin by downloading and installing Tor Browser. Once the installation is complete, click Finish, and Tor will launch for the first time. You'll be greeted with a settings dialog used to control how you connect to the Tor network. Typically, you can click the Connect button, but if you use a proxy to connect to the internet, you'll need to click the Configure button to enter your settings.

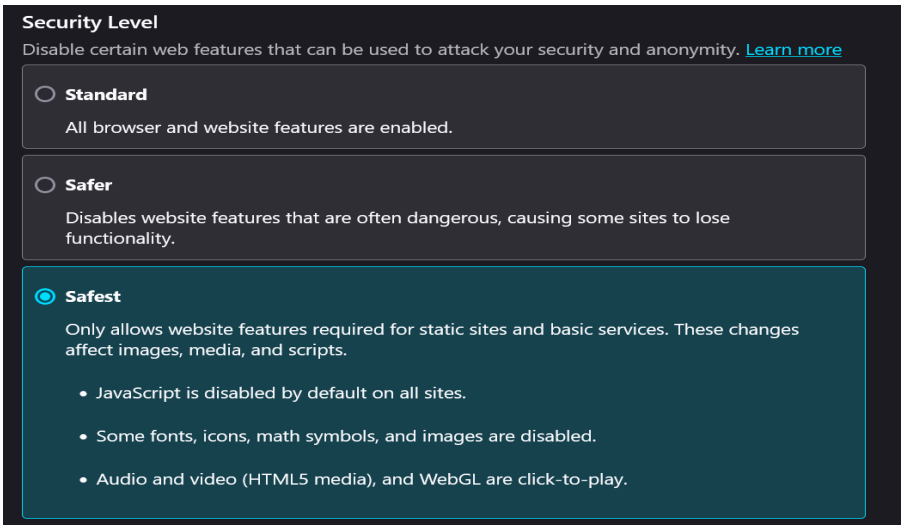
Get Online with Tor

There might be a slight delay while Tor sets up the connection to the network through relays. The browser will inform you that the initial connection might take a few minutes. Once the connection is established, the Tor Browser will open and be ready to use. Since Tor uses the same underlying code as Firefox, if you've used Mozilla's

browser before, it should feel quite familiar. Even if you haven’t used Firefox, you’ll find Tor’s interface very similar to other browsers like Edge, Chrome, and Safari.

Choose Your Security Level

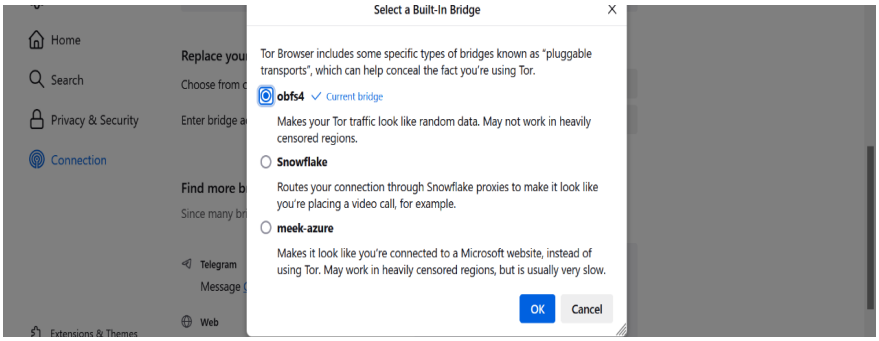
Before you start, it's important to note that using Tor involves a balance between privacy/security and convenience. By default, security is set to Standard, which is still far more secure than other browsers. To enhance security, click on the onion symbol next to the address bar and select Security Settings. Use the Security Level slider to adjust your preferred level of protection.



Change Your Browsing Habits

To get the most out of Tor, you'll need to adjust a few of your browsing habits. The first change is the search engine you

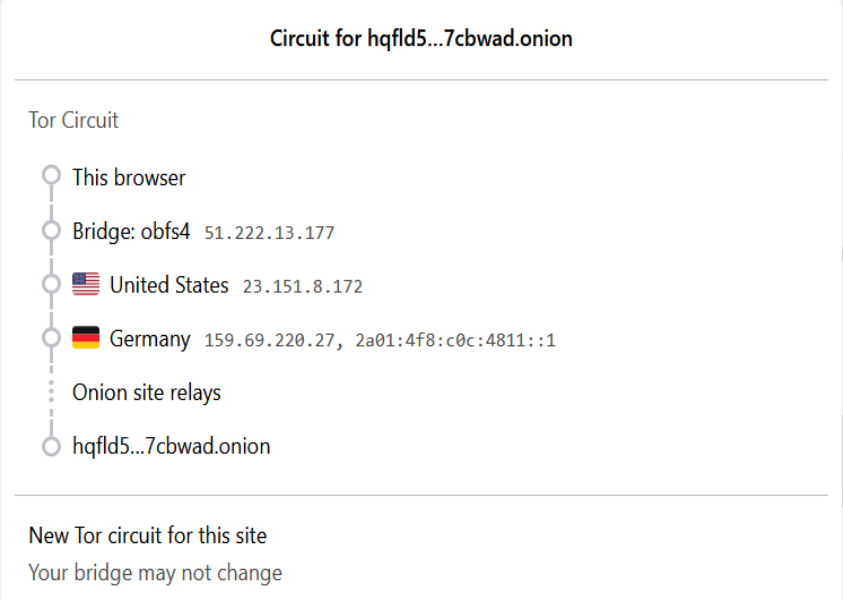
use. Instead of relying on Google or Bing, it's recommended to use Disconnect.me, a search engine that prevents trackers from monitoring your activity. You can use it with Bing, Yahoo, or DuckDuckGo. Additionally, it’s advised to avoid installing browser extensions, as these could compromise your privacy by leaking information.



Understand Tor Circuits

As you browse the internet, Tor keeps your activities safe by avoiding direct connections to websites. Instead, your connection is bounced around between various nodes in the Tor network, each hop anonymizing your identity. This process makes it extremely difficult for a website to track who and where you are, but it also contributes to slower browsing speeds.

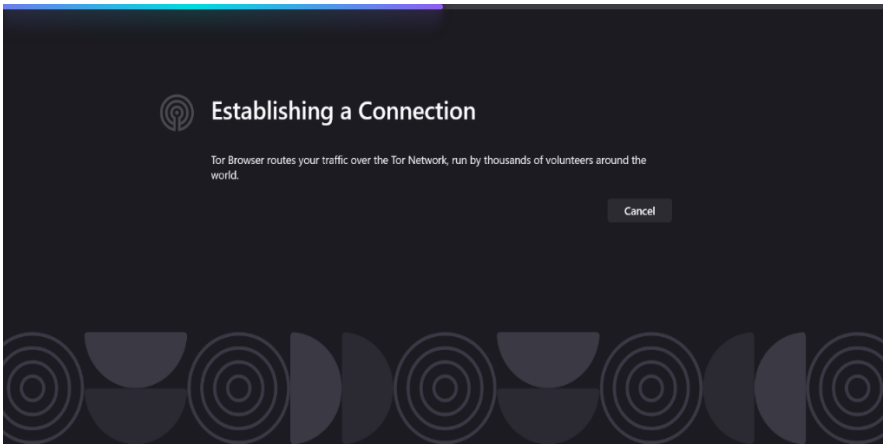
If you experience significantly slow performance or a page stop responding, you can start a new Tor circuit by clicking the hamburger icon and selecting the **‘New Tor Circuit for this Site’** option. This will force Tor to find a new route to the site.



Create a New Identity

The “New Circuit” option only applies to the current tab. If you want an even higher level of privacy, you can click the hamburger icon and select ‘New Identity,’ which will close and restart Tor with a new IP address.

When you connect to a site through Tor, you may see a pop-up warning that a particular website is attempting to track you. How often these warnings appear depends on the sites you visit and the privacy settings you have chosen.



Use HTTPS

To remain safe and anonymous online, it's essential to use HTTPS instead of HTTP versions of websites. Tor Browser comes with the HTTPS Everywhere extension pre-installed, which will automatically redirect you to the secure version of any website, if available. However, always pay attention to the address bar for added protection. If you are connected to a secure website, you'll see a green lock symbol. If it's absent, click the "i" icon for more information.

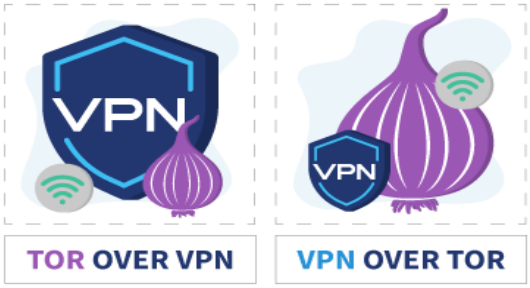
Access .onion Sites

The safest way to browse the web through Tor is by visiting .onion sites, also known as hidden Tor services. These websites cannot be indexed by search engines, and to access them, you must know the exact address. There are various .onion directories available to help you find such sites, but proceed with caution. It's easy to stumble upon sites offering

illegal content, selling illicit items, or promoting criminal activity.

Try Tor Over VPN

For an additional layer of privacy, consider connecting to a VPN before launching the Tor Browser. The VPN won't be able to see your activity within Tor, and it adds the benefit of preventing any Tor relay from viewing your real IP address. It also keeps your ISP from knowing that you're using Tor, which can be helpful if Tor is blocked in your region.



Conclusion

There is no single anonymity network that does everything. To ensure effective anonymity, you must combine multiple

tools. Even if you manage to use all three networks properly, there’s still more to learn. Each network serves its unique purpose.

There are many more tools that can work with these networks to provide even greater functionality, including advanced SSH tunnelling and configuration, personal VPNs, and numerous command-line utilities. When used together, these tools can achieve far more than what most users can do with simple GUI-based software. Anonymity networks today are similar to the internet in the early 1990s—a "realm of hackers" working towards a better future.

Chapter 8

DARK WEB FOR YOUR OSINT

📜 **“"*In the depths of the Dark Web, intelligence isn’t found—it’s uncovered.*"**

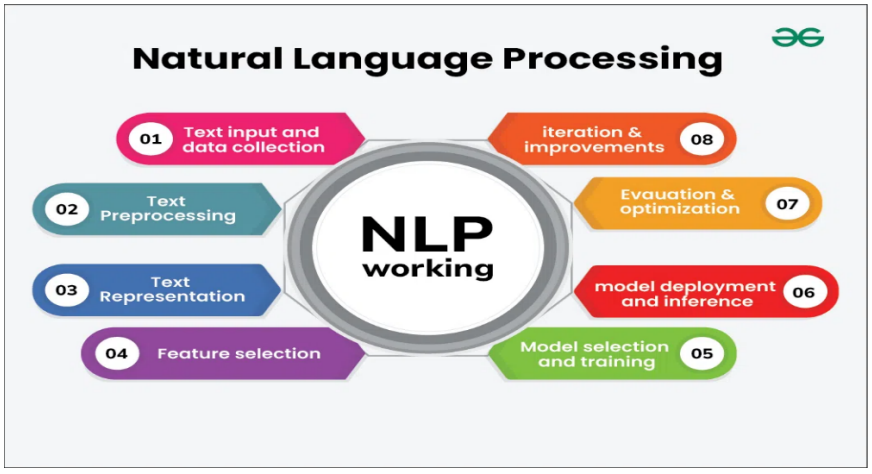
Law enforcement, journalists, and analysts use OSINT techniques to track hidden activities.

Are You Tracking Information Leaks About the Dark Internet?

When your job is to protect people and resources, the Dark Internet (or Darknet) becomes a critical area to explore. Darknet information plays a crucial role in safety and threat intelligence. The team at Echoes has developed an OSINT tool, Beacon, to search the dark net efficiently. With Beacon, you can sift through the vast and often disorganized data to extract meaningful intelligence relevant to your organization.

The Solution - A Dark Search Engine

Beacon is an advanced dark net search tool that indexes multiple sources, including websites, code repositories, and databases. Developed by Echoes, a leader in data discovery, Beacon provides structured intelligence from the dark net. Unlike Echoes, which focuses on real-time data, Beacon specializes in historical data, offering users a deeper insight into hidden information.



Using Natural Language Processing (NLP), Beacon extracts key entities from dark web data, such as names, locations,

organizations, phone numbers, and social security numbers. By creating an internal knowledge graph, Beacon enables analysts to track information across various platforms, including social media and underground forums.

How Can You Use This Information?

Organized dark net data allows analysts to make informed decisions about potential threats. **For example:**

Brand Protection: Identify stolen email addresses, NDA violations, classified leaks, or counterfeit products.

Executive Security: Detect leaked information, including hacked emails and compromised social media accounts.

Retail Loss Prevention: Track illegally sold products and identify unauthorized sellers.

Corporate Security: Uncover NDA breaches and leaked corporate data.

Insurance & Legal Compliance: Monitor leaked information to mitigate legal liabilities and manage PR crises.

Financial Fraud Prevention: Detect leaked credit cards, reused passwords, and compromised banking details.

Cybercrime Tracking: Understand underground activities and identify emerging threats.

Unveiling the Dark Internet

Beacon simplifies dark net data by structuring vast amounts of unfiltered information. This OSINT tool quickly identifies valuable intelligence within the depths of the dark web, helping professionals stay ahead of potential threats. Cybercriminals frequently exploit dark net vulnerabilities, distributing trepanised software such as malicious Tor Browser versions. These modified browsers have been used to steal over $40,000 in Bitcoin. Criminals create deceptive websites mimicking the official Tor Browser page, tricking users into downloading malware-infested versions.

How Cybercriminals Operate on the Dark Web

Malicious Domains: Cybercriminals set up fake websites like "topolect [.] org" to deceive users into downloading trojanized browsers.

Distribution Tactics: They spread malware through spam messages on Russian forums, promoting fake Tor updates.

SEO Manipulation: Criminals use search engine optimization (SEO) tactics to push their malicious pages higher in search rankings.

Social Engineering: Fake messages claim that using their version of Tor will ensure anonymity and bypass government censorship.

Payload Injection: The trojanized Tor Browser silently injects malicious JavaScript that tracks users and steals sensitive data.

Understanding the Deep Web, Dark Web, and Darknet

The internet consists of multiple layers:

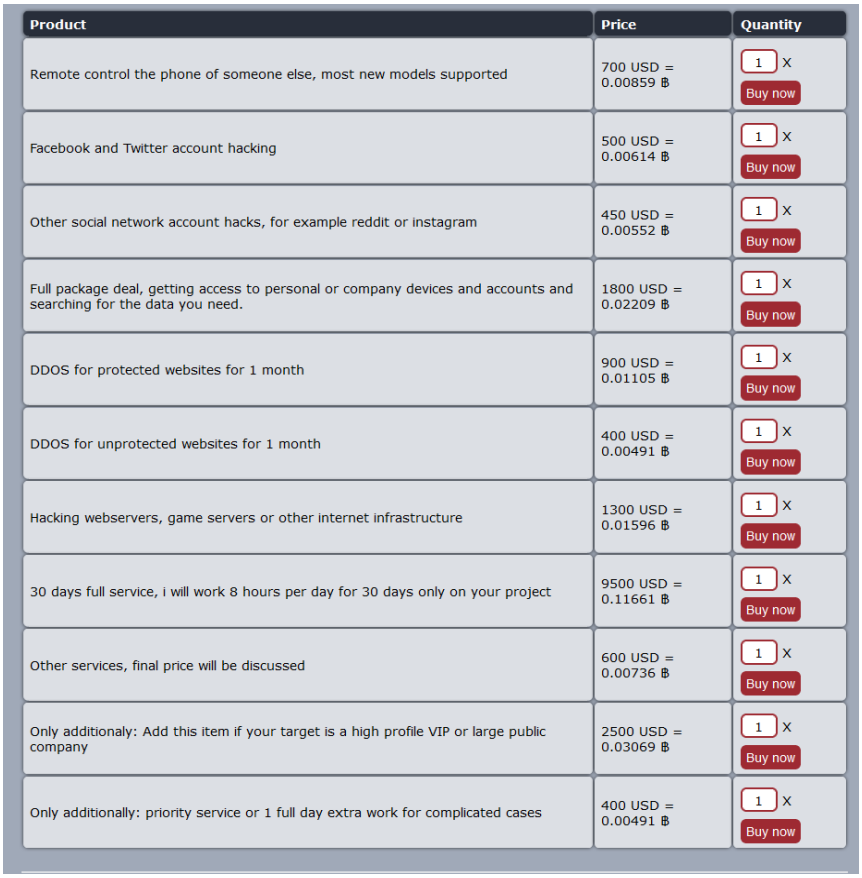
Surface Web: The visible part of the web indexed by search engines like Google (e.g., Facebook, Wikipedia, news sites). This makes up only 4-6% of the total web.

Dark Web: An encrypted network accessed via special software like Tor, used for anonymous communication and hidden services.

Darknet: A subset of the dark web, facilitating illicit activities like drug trade and cybercrime markets.

Is the Darknet Only for Criminals?

Although the dark web has a notorious reputation, it also serves legitimate purposes. Whistleblowers, journalists, and activists use it to protect their identities from oppressive regimes. Governments and cybersecurity professionals leverage it for intelligence gathering and threat analysis. However, the presence of illegal markets, such as the infamous Silk Road, underscores the need for vigilant monitoring and security measures.



Product	Price	Quantity
Remote control the phone of someone else, most new models supported	700 USD = 0.00859 ฿	1 X Buy now
Facebook and Twitter account hacking	500 USD = 0.00614 ฿	1 X Buy now
Other social network account hacks, for example reddit or instagram	450 USD = 0.00552 ฿	1 X Buy now
Full package deal, getting access to personal or company devices and accounts and searching for the data you need.	1800 USD = 0.02209 ฿	1 X Buy now
DDOS for protected websites for 1 month	900 USD = 0.01105 ฿	1 X Buy now
DDOS for unprotected websites for 1 month	400 USD = 0.00491 ฿	1 X Buy now
Hacking webservers, game servers or other internet infrastructure	1300 USD = 0.01596 ฿	1 X Buy now
30 days full service, i will work 8 hours per day for 30 days only on your project	9500 USD = 0.11661 ฿	1 X Buy now
Other services, final price will be discussed	600 USD = 0.00736 ฿	1 X Buy now
Only additionaly: Add this item if your target is a high profile VIP or large public company	2500 USD = 0.03069 ฿	1 X Buy now
Only additionally: priority service or 1 full day extra work for complicated cases	400 USD = 0.00491 ฿	1 X Buy now

Beacon equips professionals with a powerful tool to uncover crucial information hidden within the dark net. Whether for corporate security, fraud prevention, or cybercrime investigation, structured OSINT intelligence is essential for staying ahead in the digital age.

Chapter 9

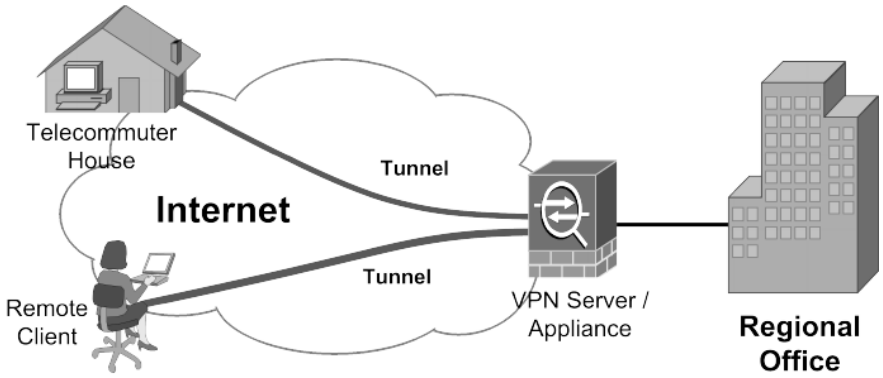
ALL ABOUT VPN

📜 **“"*A VPN is your first shield in the digital battleground—use it wisely.*"**

Not all VPNs are equal—choosing the right one can make or break your anonymity.

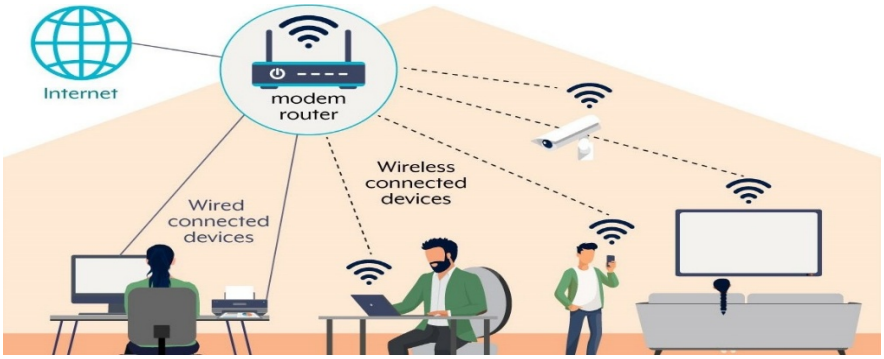
A Virtual Personal Network (VPN) provides you with online anonymity and privacy by creating a private network over a public internet connection. VPNs hide your internet protocol

(IP) address, making your online activities nearly untraceable. Most importantly, VPN services set up encrypted and secure connections to offer better privacy than a shared Wi-Fi hotspot.



Why would you need a VPN service?

Surfing the web or transacting on an unsecured Wi-Fi network means you could be exposing your personal info and browsing habits. That’s why a Virtual Private Network (VPN) should be a must for anyone concerned about online privacy and security. Unless you're logged into a private Wi-Fi network that requires a password, any data sent during your session might be exposed to eavesdroppers using the same network. VPNs protect your email, online shopping, or paying bills by encrypting your connection and keeping your online activity anonymous.



How VPN protects your IP address and privacy

VPNs create an information tunnel between your local network and an exit node located miles away, making it appear as if you're in a different location. This advantage allows for online freedom, such as accessing your favorite websites or apps while on the go.

VPNs use encryption to scramble data when it’s sent over a Wi-Fi network, making it unreadable to hackers. This is especially important when using a public Wi-Fi network, as it prevents anyone on the same network from eavesdropping on your online activity.

VPN Privacy: What does a VPN conceal?

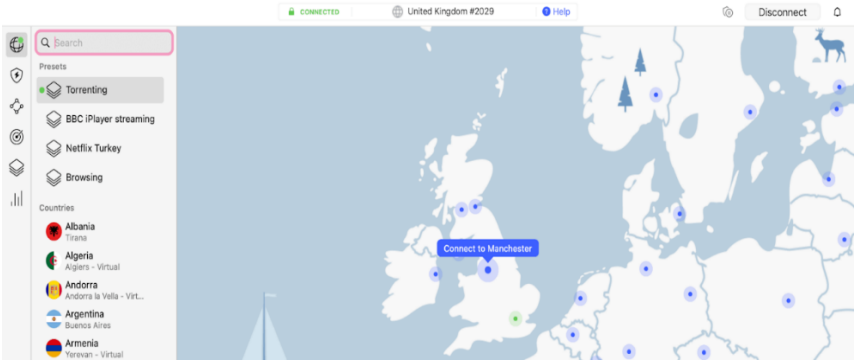
A VPN can conceal a lot of information that might jeopardize your privacy. Here are five examples:

1. Your browsing history

Your ISP and browser can track what you do online. Without a VPN, your browsing history could be sold to advertisers. With a VPN, your online activities are concealed.

2. Your IP address and location

Anyone who gets your IP address can determine your online activity and location. A VPN helps hide your actual IP address, keeping your browsing activity anonymous.



3. Your location for streaming

Streaming services sometimes restrict content based on location. A VPN allows you to access content as if you were in your home country, bypassing these restrictions.

4. Your devices

A VPN secures your devices (laptop, tablet, smartphone) from hackers, especially when connected to public Wi-Fi networks.

5. Your internet activity to keep net freedom

A VPN prevents your ISP from monitoring your online activity and helps protect your freedom to browse privately.

How does a VPN help safeguard against identity theft?

Identity theft happens when thieves steal personal data and use it for fraudulent activities. A VPN helps protect your information by encrypting it, creating a secure tunnel for your data that cybercriminals cannot access.

What should you look for in VPN services?

When searching for a VPN, consider your needs and priorities. Do you want to browse anonymously, protect your data on public Wi-Fi, or access content from home while traveling? Here are some things to look for in a good VPN:

How to Select a VPN

Here are questions to ask when choosing a VPN provider:

1. Do they respect your privacy?

Ensure the VPN provider has a no-logs policy, meaning they don't track your online activities.

2. Do they use the latest encryption protocols?

Look for VPNs that use OpenVPN, which provides stronger security than older protocols like PPTP.

3. What are the data limits?

Ensure the VPN provides adequate bandwidth and doesn’t impose data caps that could slow you down.

4. Where are the servers located?

Check if the VPN provider has servers in the countries you want to connect to.

5. Can you install it on multiple devices?

Check whether the VPN allows you to use it on multiple devices at once, such as phones, tablets, and computers.

	ExpressVPN	NordVPN	IPVanish	TunnelBear	CyberGhost	Private Internet Access
Simultaneous Connections	3	6	10	5	5	5
Number of Servers	1,700	4,873	1,000 +	350 +	2,700	3,252
Servers across the Globe (countries)	148	62	60 +	20	60	37
Number of IP addresses	15,000	5,000	40,000 +	n/a	n/a	n/a
Kill Switch	✓	✓	✓	✓	✓	✓
No Logs Policy	✓	✓	✓	✓	✓	✓
Free Version	✗	✗	✗	✓	✗	✗
Bitcoin payment	✓	✓	✗	✓	✓	✓
Country/ Jurisdiction	British Virgin Islands	Panama	United States	Canada	Romania	United States

6. VPN Glossary

Understanding VPN terminology can be tricky, so here's a glossary of common terms:

Chapter 10

SECURITY IMPACT

📜***""The Darknet challenges the very fabric of cybersecurity—where innovation and threats evolve in tandem."***

As cybersecurity strengthens, the Darknet finds new ways to adapt an endless game of cat and mouse.

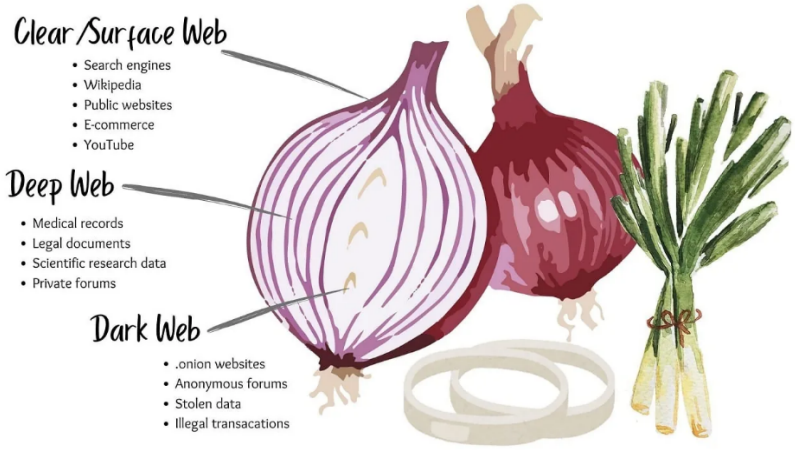
Not to be mistaken with the entire deep web, the darknet is a collection of thousands of sites that cannot be accessed through ordinary means and are not indexed by search engines such as Google or Yahoo. In other words, the darknet is an overlay of networks that require specific tools and applications for access. The history of the darknet predates the 1980s, with the term initially used to describe computers on ARPANET that were hidden and programmed to receive messages without responding or acknowledging anything, thus remaining undetectable or "in the dark." Since then, "darknet" has become an umbrella term referring to hidden sections of the internet or networks deliberately concealed from public view.

Paradoxically, the darknet's development can be partially credited to the U.S. military. The most common way to access the darknet is through tools like the Tor network. The routing techniques used by Tor were developed in the mid-1990s by mathematicians and computer scientists at the U.S.

Naval Research Laboratory to protect U.S. intelligence communications online.

USE AND ACCESS

The applications of the darknet are as diverse as the internet itself, including email services, social media, file sharing, news websites, and e-commerce. Accessing it requires specialized software, configurations, or permissions, often using nonstandard communication protocols and interfaces. Currently, two of the most well-known ways to access the darknet are through overlay networks: Tor and I2P.



Tor, short for "**The Onion Router,"** was primarily designed to keep users anonymous. Just like the layers of an onion, data is wrapped in multiple layers of encryption. Each layer reveals another relay until the final layer sends the data to its destination. Information is sent bidirectionally, meaning data is transmitted back and forth through the same tunnel.

On any given day, over a million users are active on the Tor network.

I2P, or the Invisible Internet Project, was designed for user-to-user file sharing. It encapsulates data in multiple layers, similar to a garlic clove, grouping multiple users' data together to prevent decryption and analysis. It transmits data through a unidirectional tunnel.

WHAT'S OUT THERE?

As mentioned earlier, the darknet hosts news sites, e-commerce platforms, email services, and hosting solutions. While many of these services are legitimate alternatives to mainstream platforms, a significant portion is associated with illegal activities due to its anonymous nature. Since the 1990s, cybercriminals have used the darknet as a space to communicate, coordinate, and now even

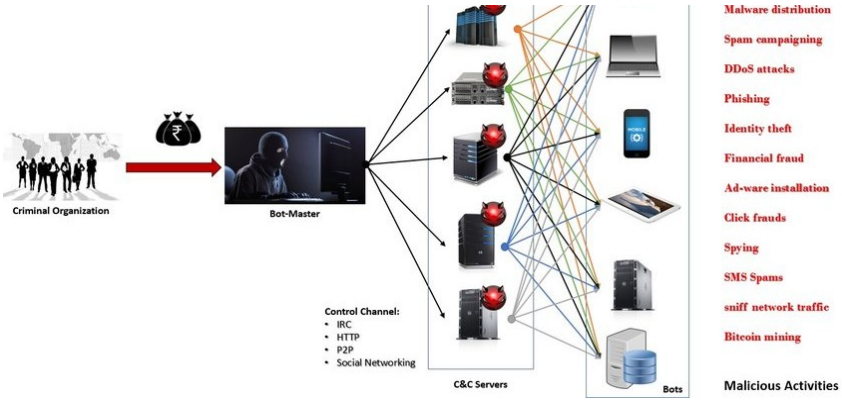
One of the most common darknet services is encrypted email, which has seen a dramatic increase in usage, coinciding with the rise of ransomware. Cybercriminals often

use these email services to execute attacks while avoiding detection by authorities. Another critical service is darknet hosting. Just as cloud computing is used by businesses for IT infrastructure, cybercriminals leverage darknet hosting for illicit websites, e-commerce marketplaces, and DDoS-for-hire services. However, these hosting services are often unstable, as law enforcement or vigilante hackers may take them down for political, ideological, or ethical reasons. Forums also serve as meeting places where hackers and criminals exchange knowledge, plan attacks, and refine cyberattack techniques. These forums include specialized discussions in multiple languages and may be associated with specific hacking groups, attack vectors, or ideological movements.

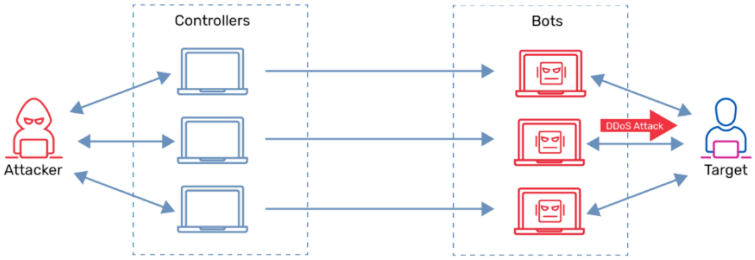
Finally, just like the surface web, the darknet has search engines such as Candle and Torch, which allow users to find and navigate various forums, websites, and marketplaces.

A DIGITAL STORE

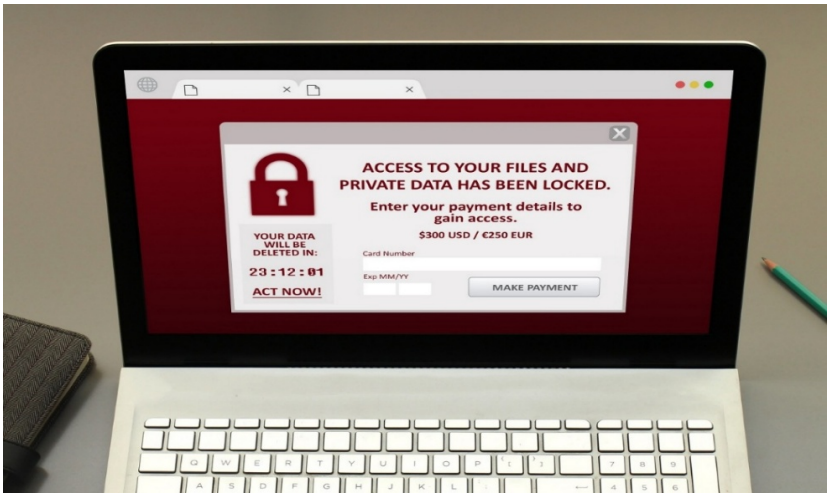
Perhaps the most concerning aspect of the darknet is the rise of e-commerce sites that facilitate cybercrime. These platforms have gained immense popularity in recent years due to the increasing availability of DDoS-for-hire and botnet rental services, which allow non-technical users to launch sophisticated cyberattacks.



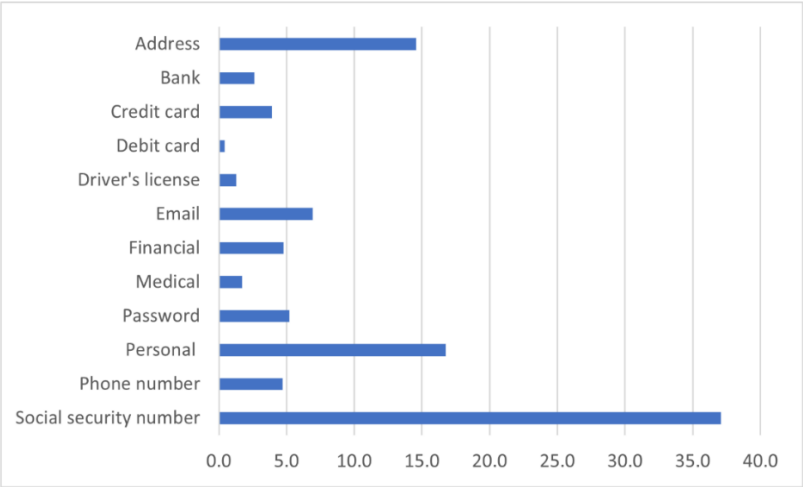
Many offer intuitive, graphical interfaces that make launching an attack as simple as placing an order online. One example is Putin Tresser, a DDoS-for-hire service that provides various attack options, detection evasion tools, and even customer support. Another example is the Jex botnet, discovered in 2018, which exemplifies the growth of botnet rental services.



Prices for these services range from as little as $100 to thousands of dollars, depending on factors such as the number of attack vectors, attack size (Gbps/Tbps), and market demand. Similar to botnets and DDoS services, ransomware-as-a-service models allow users to launch attacks with minimal effort, simply selecting a ransom amount and customizing the ransom note before deploying malware.

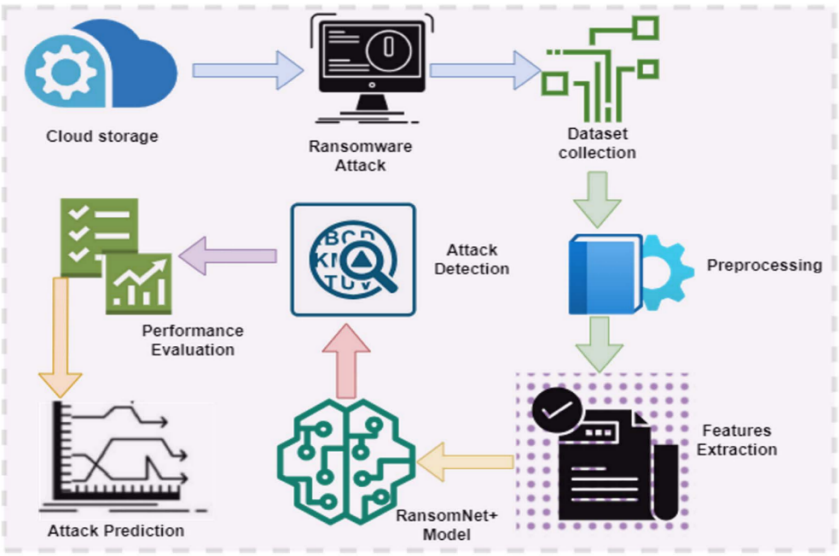


Hackers-for-hire services are also widely available. Users can pay for services ranging from hacking email and social media accounts to designing custom malware



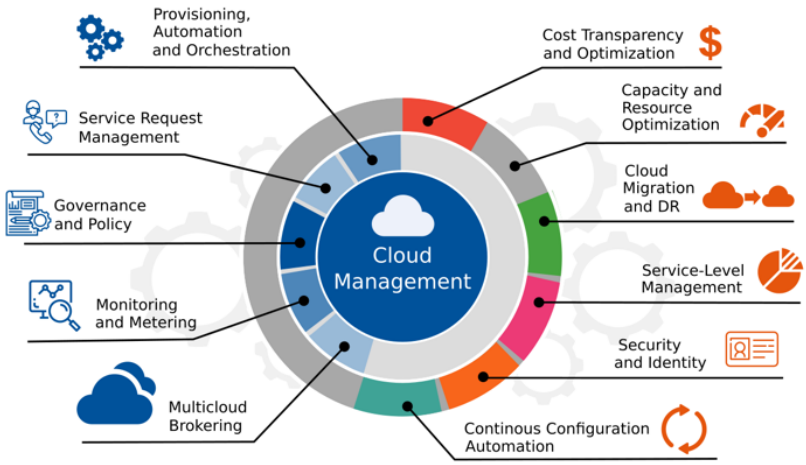
CAN CLOUD PROTECT AGAINST RANSOMWARE?

Ransomware encrypts victims' files and demands a Bitcoin ransom for decryption. While cloud storage provides a convenient and cost-effective alternative to off-site backups, it is not inherently protected from ransomware attacks. One of the biggest advantages of the cloud is its security infrastructure. While cloud providers are high-profile targets, they invest heavily in cybersecurity measures to protect against attacks. To defend against ransomware in cloud environments, businesses must understand the shared responsibility model of cloud computing.



The Fastest Way to Cloud Ransomware Protection

Using the cloud for backups is effective, but instead of relying on a single cloud provider, utilizing multiple clouds simultaneously can enhance security and minimize risks—without significantly increasing costs. A dedicated cybersecurity and disaster recovery plan is crucial when leveraging the cloud. By assessing your baseline cybersecurity posture, you can identify vulnerabilities and mitigate threats more effectively. Taking the time to categorize your applications helps determine Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), leading to a more focused disaster recovery strategy. Our team of experts specializes in backup solutions, disaster recovery, and cybersecurity, ensuring a seamless cloud transition.



Is USENET Part of the Deep Web?

The terms Deep Web, Dark Web, and similar phrases have been widely discussed in the media. Notably, the hacker collective Anonymous has taken down several Dark Web sites involved in illicit activities. This has sparked curiosity about the Deep Web and how it differs from USENET.

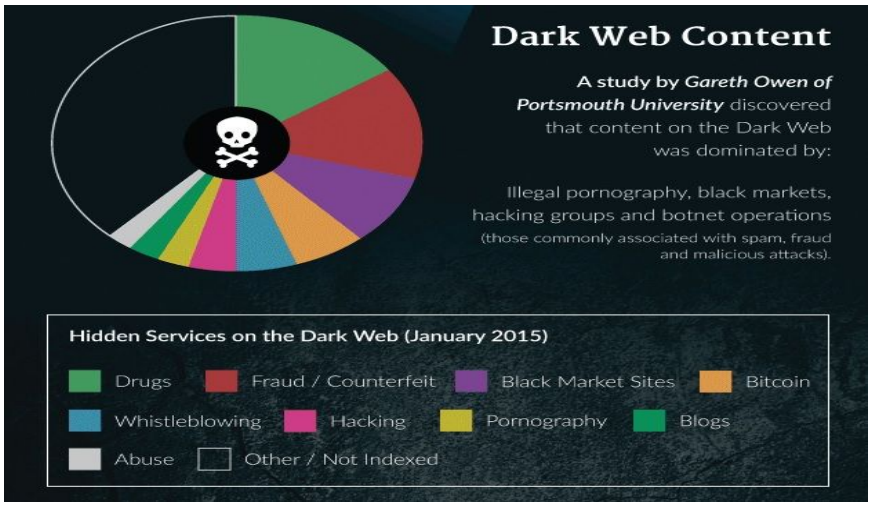
Understanding Indexing

You may have encountered terms like "search engine optimization" (SEO), which involves techniques to make websites more discoverable by search engines. Websites are indexed when search engines find them through links or direct submissions. However, some sites never get indexed, forming what is known as the Dark Web. In contrast, USENET functions differently. It doesn’t require search engine indexing because it operates as a distributed network of newsgroups rather than traditional websites.

Not Everything Unindexed is Sinister

Many unindexed sites exist for legitimate reasons. Academic research pages, internal databases, and private web portals may not be intended for public discovery. Additionally, abandoned websites, forgotten by their creators, can also become part of the Dark Web. While some Dark Web sites facilitate illegal activities, stumbling upon them accidentally is highly unlikely.

USENET, on the other hand, is a transparent platform designed for sharing information rather than concealing it. While it hosts a vast archive of discussions, it remains an open and accessible resource.



Protecting Your Computer from Cyber Threats

Many people worry about government surveillance, yet willingly share their personal data on social media. Platforms like Facebook, Instagram, and Twitter collect and store vast

amounts of user data, often making it readily available for advertisers—and potentially malicious actors.

Cybercriminals can extract this information, potentially revealing your location and habits. Even beyond social media, your online activity is constantly being tracked. Have you ever emailed a friend about vacation plans, only to find travel ads flooding your inbox? That’s because companies like Google analysis your emails and browsing habits to serve targeted advertisements. To enhance privacy, consider using browser extensions like **DoNotTrackMe** and **Self-Destructing Cookies**. These tools limit tracking and prevent companies from collecting excessive data.

Enterprise-Level Security Risks

While personal security is important, businesses face even greater risks. Recent data breaches at major retailers like Home Depot and Target have compromised millions of credit card details. Often, hackers don’t bypass firewalls directly but exploit human errors through phishing emails,

compromised third-party vendors, or even rogue employees plugging in infected USB drives. Cybercriminals also operate on the Dark Web, selling stolen data and hacking tools. Accessing these marketplaces requires special browsers like Tor, making them difficult to trace. To mitigate risks, businesses must invest in cybersecurity audits, penetration testing, and employee training. Ignoring these measures until after a breach can lead to devastating consequences.

The Danger of Unverified Software Updates

Every day, you receive prompts for software updates—on your phone, computer, and even smart devices. But do you ever question what's being installed? Malicious actors can disguise malware as legitimate updates, allowing them to hijack cameras, microphones, and data without the user's knowledge. The lesson? Never blindly trust an update. Always verify the source before installing new software.

The Rising Threat of Cybercrime

Cybercrime, alongside global health crises and terrorism, is one of the greatest threats to modern society. Yet many businesses hesitate to invest in robust security measures until they become victims. Firewall upgrades, antivirus

subscriptions, and security training should be seen as essential investments rather than optional expenses. Educating employees on safe internet practices, including recognizing phishing scams and avoiding untrusted networks, can significantly reduce security vulnerabilities. In an era where data is as valuable as currency, proactive cybersecurity measures are no longer optional—they're a necessity.

Final Thoughts

The deep web and darknet are vast, complex spaces that go far beyond their reputation as hubs for cybercrime. While they host many illicit activities, they also provide valuable tools for privacy and secure communications. For professionals in cybersecurity and threat intelligence, monitoring the darknet is essential. It helps identify leaked credentials, potential cyberattacks, and emerging threats before they escalate. However, navigating this hidden world requires caution, awareness, and the right protective

measures. By understanding the structure of the deep web and darknet, individuals and organizations can make informed decisions—whether it’s safeguarding data, preventing cyber threats, or leveraging anonymous networks for ethical purposes.

.....

ACKNOWLEDGMENTS

Writing this book has been an **unforgettable** journey, filled with long nights, endless research, and moments of **doubt**. At times, I questioned whether I had the energy to continue, but my fascination with the **hidden world** of the dark web kept pulling me back. Curiosity is a relentless force, and this book is a testament to the need to **explore**, question, and uncover what lies beneath the surface.

I am deeply grateful to the **cybersecurity experts**, ethical hackers, and digital explorers who have, knowingly or unknowingly, inspired me to keep learning. To the online communities that challenged my understanding, thank you for pushing me to dig deeper.

And most importantly, to you, the **reader**. Whether you picked up this book out of curiosity, a thirst for knowledge, or a desire to understand the **unseen side** of the internet, I appreciate you more than words can express. Writing a book is one thing, but having someone take the time to read it is what truly makes it worthwhile.

Thank you for being part of this journey. Stay curious, stay safe, and never stop exploring

Faisal .J

ABOUT THE AUTHOR

Muhammad Faisal is a researcher and writer from Lahore, Punjab, Pakistan, with a deep interest in **cybersecurity, privacy, and the hidden layers of the internet**. Through extensive independent research, he explores complex digital topics and presents them in a way that is accessible to readers.

When not writing, he enjoys learning about **emerging technologies** and staying up to date with the latest cybersecurity trends.

Support My Work

If you found this book valuable and would like to support my research and future writing, you can contribute via Patreon:

Patreon:

patreon.com/MuhammadFaisal0317

Your support is greatly appreciated!

For inquiries, feel free to reach out via email: **faisaljalvi0509@gmail.com**