Introduction to the Dark Web

1) **What is meant by dark web?**

The dark web is the hidden collective of internet sites only accessible by a specialized web browser. It is used for **keeping internet activity anonymous and private**, which can be helpful in both legal and illegal applications.

2) **What is dark web in simple words?**

The dark web refers **to encrypted online content that is not indexed by conventional search engines**. Sometimes, the dark web is also called the dark net. ... Many dark web sites simply provide standard web services with more secrecy, which benefits political dissidents and people trying to keep medical conditions private.

3) **Can I access dark web?**

All you have to do is download a dark web browser, like **the Tor browser**. Once you install a dark web browser on your device, it functions just like a regular browser: type in a URL, and off you go. However, finding the material you're looking for on the dark web is more difficult than using a search engine like Google.

4) **What is illegal on the dark web?**

The type of content that has the most popularity on the dark web is illegal pornography, more specifically, **child pornography**. ... There is regular law enforcement action against sites distributing child pornography – often via compromising the site and tracking users' IP addresses

5) **Why do people use the Dark Web?**

The Dark Web may be used by **people wishing to carry out illegal activities online, such as selling weapons or drugs**. These kinds of operations, and the websites offering them, are often referred to as Hidden Services (above).

6) **Is Tor illegal?**

While **Tor itself isn't illegal**, you could get flagged for suspicious activity if someone discovers that you're using it. Tor Browser operates on a totally different system from that of a VPN, and protects your privacy in a highly unique way.

7) **How do you download Tor?**

For Windows:

Navigate to the Tor Browser download page.

Download the Windows .exe file.

(Recommended) Verify the file's signature.

When the download is complete, double click the .exe file. Complete the installation wizard process.

https://tb-manual.torproject.org/installation/

8) **How does dark web look like?**

Dark web sites look **pretty much like any other site**, but there are important differences. ... co, dark web sites end in . onion. That's “a special-use top level domain suffix designating an anonymous hidden service reachable via the Tor network,” according to Wikipedia.

9) **Can you access the dark web on a phone?**

Can I access the Dark web on my phone? **Yes, Android and iOS devices have Tor apps made for mobile devices**. They provide the same functionality as their desktop counterparts.

10) **Can police track Tor?**

There is no way to track live, encrypted VPN traffic.

Using the Tor browser could be suspicious to your ISP and, therefore, to the police.

11) **How do you use Tor?**

Here are the steps you need to follow in order to install and use Tor Browser.

A) Install and configure Tor Browser. Start by downloading and installing Tor Browser. ...
B) Get online with Tor. ...
C) Choose your security level. ...
D) Rethink your browsing habits. ...
E) Understand Tor circuits. ...
F) Create a new identity. ...
G) Use HTTPS. ...
H) Access .

12) [How to protect your privacy online with Tor Browser | TechRadar]

13) Are there loan sharks on the dark web?

6 days ago

The dark web is a place where black market activity and illegal things happen online. It's a part of the Internet that is set up by hackers, loan sharks, and other unscrupulous parties who are trying to find a way to get away with their illegal activities.

14) What are .onion sites?

A top level Internet domain used by anonymous websites on the Dark Web. Access to onion sites is via the Tor browser. See Dark Web, Tor and OnionLand Search Engine. Onion Website Addresses. Hardly user friendly, onion addresses are not registered with the Internet's domain name system (see DNS).

https://www.pcmag.com/encyclopedia/term/onion-domain

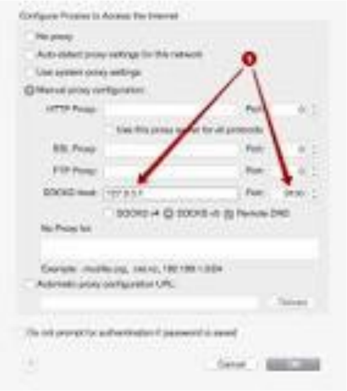
15) Is Tor free?

Tor, short for The Onion Router, **is free and open-source software** for enabling anonymous communication.

16) What is so scary about the dark web?

Stolen information – This is where stolen information from data breaches and/or stolen identities end up. Think Social Security numbers, personal info, and banking logins. You can even buy login information for services like Netflix and Amazon Prime on the dark web.

17) How do I set up Tor?



Configure Proxies to Access the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy: Port: 0
□ Use this proxy server for all protocols
SSL Proxy: Port: 0
FTP Proxy: Port: 0
SOCKS Host: 127.0.0.1 Port: [illegible]
○ SOCKS v4 ● SOCKS v5 ☑ Remote DNS

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

□ Do not prompt for authentication if password is saved

Recommended use Tor Browser

A) Recommended use Tor Browser. ...
B) Click Security Settings.
C) Set the security level: ...
D) Tor Browser is ready for use, and you can immediately begin to surf anonymously. ...
E) Install the program Proxifier. ...
F) Select the Network Settings.
G) See use the local IP address and port of the Tor network connection.

18) Does Tor hide your IP?

Tor is a free software program that you load onto your computer (like a browser) that **hides your IP address every time you send or request data on the Internet**. The process is layered with heavy-duty encryption, which means your data is layered with privacy protection.

19) Who is the owner of Tor?

The Tor Project, Inc. Tax ID no. The Tor Project, Inc. is a Seattle-based 501(c)(3) research-education nonprofit organization founded by **computer scientists Roger Dingledine, Nick Mathewson and five others**. The Tor Project is primarily responsible for maintaining software for the Tor anonymity network.

20) Do you need VPN for Tor?

You'll **need a VPN service and the Tor Browser**. If you want to route all of your traffic through Tor, you can use tools like Tortilla. This tool will route all your web traffic through Tor nodes. However, in most cases, you'll likely be using the Tor Browser.

21) What is illegal Tor?

In TOR the data is encrypted in layers analogous to the layers of an onion. TOR through encryption keeps the identities and IP addresses of the people accessing the Dark web untraceable. ... **Simply surfing on the Dark web is not illegal**, unless illegal content is accessed.

22) Why is my Tor so slow?

Why Is Tor Slow? **Tor is inherently slower compared to other browsers**. The main reasons include the absence of a direct connection between the client and online service and, conversely, the presence of several intermediary layers to facilitate routing.

Summary:

A Complete Look at the World Wide Web

If the Internet that we can all access only makes up a very small percentage of the entire Internet, what is hosted on the rest of it? In what is known as the "**Deep Web**", most of the Internet is filled with legitimate data; mostly in the form of unindexed content. Data that is encrypted such as online banking, pay-to-play video services, and other forms of everyday Internet use make up a large portion of the **Deep Web**. With the revelations that there was an online black market where people could get almost anything, many people started confusing the deep web with the dark web, or darknet. This misconception has many people confused about what exactly the purpose is for the seemingly bottomless Internet, but with most of it being taken up by cloud environments and other encrypted services, the notion that the Deep Web is somehow nefarious is misplaced.

What is the Dark Web?

On the other hand, the Dark Web is also hosted on the Deep Web, beyond sight of the average Internet user. While the surface web is unencrypted and able to be accessed by just about anyone who wants to use it, the Dark Web is accessed only through encrypted browsers. You may have heard of specific ransomware programs asking you to download the Tor web browser to make payments. This is because Tor is one of the web browsers able to browse the Dark Web, although it should be mentioned that it's not exclusively used for the purposes of paying ransomware demands.

Tor is what is known as an onion router. Essentially in order to maintain a user's anonymity, an onion router will pass user queries through several intermediary accounts to hide the user from being tracked. It’s like passing each command through the several layers of an onion, thus the moniker.

What Else is On the Dark Web?

The services offered on the Dark Web are varied, but they all generally have one thing in common--most of them are illegal. If you can think of it, and it’s not on the normal World Wide Web, chances are there is a place on the Dark Web for it. Some of the services provided on the Dark Web can include, but are not limited to, the following:

- Illegal pornography
- Bitcoin services (not outright illegal, but often used for money laundering purposes)
- Botnets that can be bought or purchased for nefarious use
- Markets for drugs, weapons, and other illegal contraband
- Scams and other phishing threats are rampant on the Dark Web, so even those who are looking to take advantage of these services have to be careful

Most notable for businesses is that hacking services can be acquired for even non-experienced users, meaning that anyone with an agenda has access to services that could cripple your business. It’s more important today than ever before to make sure that your organization is taking the necessary measures to protect itself from these threats.

With so much information hidden from view, there is a significant chance that there may be information out there that may end up becoming problematic for your business.

An introduction to the DarkNet

The term cybercrime usually brings to mind phishing scams, 419 scams and online banking fraud. Most people are unaware of the cyber underworld known as the DarkNet. In this hidden and mysterious virtual domain, cybercrime takes on a different dimension.

The DarkNet is a network that is deliberately hidden and inaccessible through the internet with which we are all familiar (the “surface net”). It is accessed with the help of specially designed software which anonymises users’ identity and encrypts information sent over the network.

The concept of the DarkNet was originally developed by the US Navy. However, because of the anonymity the DarkNet offers, various other groups have taken advantage of it. Journalists, political dissidents and whistle-blowers, particularly those living in repressive societies, rely on the DarkNet to publish information freely and communicate with sources, without fear of retribution.

While activists use the DarkNet to organise themselves without revealing their position to the governments they oppose, terrorists and criminals use the DarkNet for the same reason.

The DarkNet and the Deep Web

The Deep Web refers to all parts of the internet which cannot be indexed by search engines. The Deep Web therefore includes data contained in private databases and academic resources and member-only websites.

The DarkNet forms part of the Deep Web as its contents are not accessible through search engines, but the DarkNet is different in that it can be accessed by anyone with the right software.

How does it work?

The anonymising software is freely available through the surface net and makes use of ‘onion routing’ technology. The name stems from the way in which data sent over the network is encrypted at multiple layers, similar to the layers of an onion.

The most popular onion routing software is Tor (The Onion Router). Internet traffic on the DarkNet is directed by programs such as Tor, through a free, worldwide, volunteer network consisting of thousands of relays provided by volunteers.

Because no search engines work on the DarkNet, simple directories containing links to addresses are used to navigate the DarkNet. However link directories are unreliable as addresses are constantly changing. Often a website will be shut down overnight and reopened the next day at a different address, as sites are compromised by hackers or law enforcement agencies. Navigating the DarkNet is notoriously difficult for new users.

Regular users rely on website address information from other users who are already in the know.

Illegal uses of the DarkNet

A common feature of the DarkNet is its ‘virtual markets.’ The secretive nature of the DarkNet makes it ideal for transacting unlawful business and many DarkNet markets unashamedly facilitate the sale of items such as child pornography, drugs, weapons, stolen goods and assassination services. Cryptocurrencies such as Bitcoin are used as the method of payment because credit cards are not acceptable: they can be traced and transactions can be repudiated.

Corporate uses and risks

Some corporations are using the DarkNet as a safe way to communicate with employees in different locations and protect confidential business activities, relationships and databases from eavesdroppers. In certain respects, the anonymising software used to access the DarkNet may be used by a corporation in place of traditional VPN’s (Virtual Private Networks).

Traffic analysis of the surface net (internet surveillance) is a major reason why corporations (and individuals) are using Tor. Traffic analysis enables organisations or hackers to learn the behaviour and interests of subjects or groups, by following the source and destination of internet traffic. Tor and other DarkNet browsers seek to eliminate the risks of both simple and sophisticated traffic analysis by distributing transactions over several places on its network. No matter where information may be intercepted, an accurate link to a subject’s destination is virtually impossible to obtain.

What may not always be considered is that employees may be using the DarkNet to distribute information and conceal their communications. A disgruntled employee could distribute secret trade information of their employer, without the employer having any way of tracing the perpetrator. As an article in the New York Times put it “when a communication arrives from Tor, you can never know where or whom it’s from.” (New York Times Magazine, 17 December 2010). This is a risk which is potentially unknown, or at least misunderstood, by most organizations.

password
Welcome to the Darknet, where your odd proclivities are as welcome as you are

Conclusion

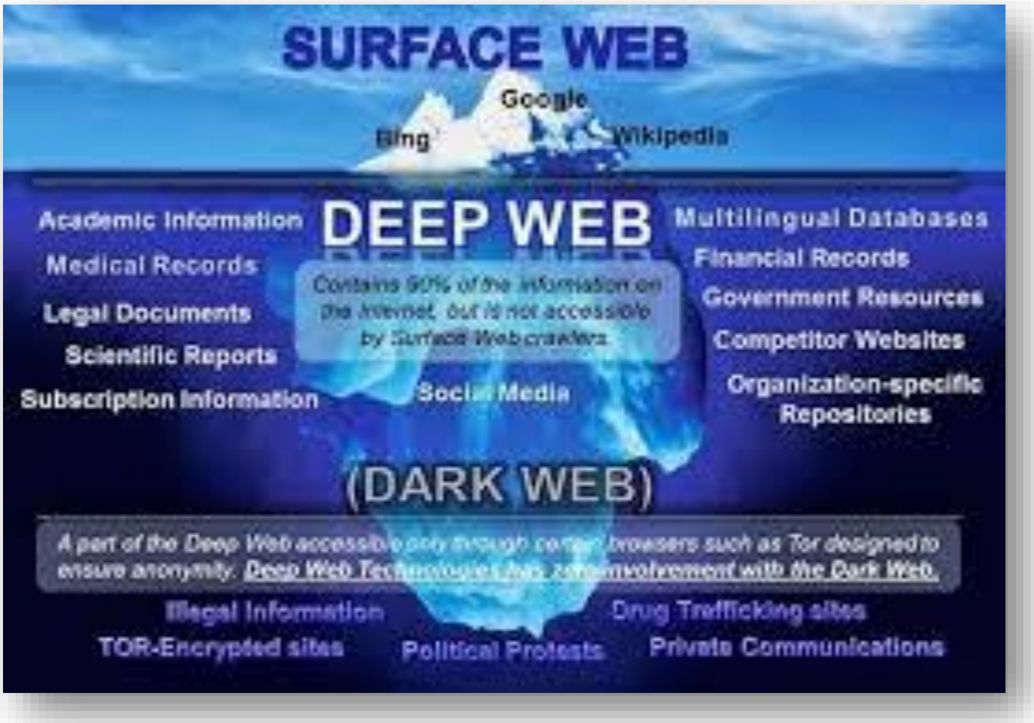
Internet surveillance of the surface net is pervasive, and may limit corporate and individual ability to communicate privately and safely online.

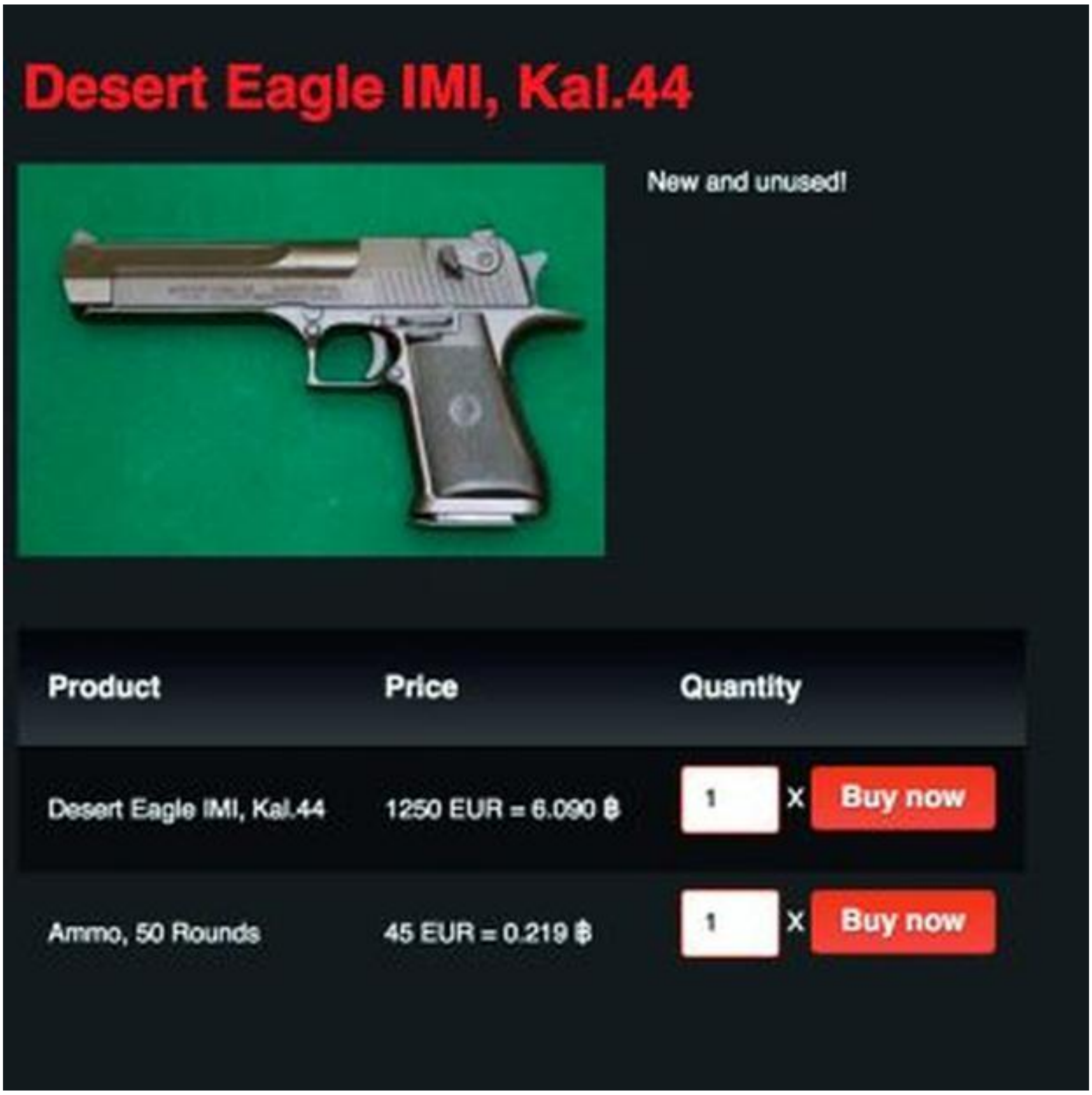
Trends in internet surveillance and hacking technology also threaten national security and infrastructure by making communication among governments, organizations, corporations and individuals vulnerable to interception and analysis.

The usefulness of the DarkNet to individuals, corporates and governments for lawful, private and secure communications is obvious, but its very secrecy lends itself to abuse by criminals. At present there is no reliable way of allowing the DarkNet to be used for good whilst barring its use for illegal purposes.

https://www.youtube.com/watch?v=BN1NU0ivzj8

https://www.youtube.com/watch?v=X2zORqBuILg





Desert Eagle IMI, Kal.44

New and unused!

Product	Price	Quantity
Desert Eagle IMI, Kal.44	1250 EUR = 6.090 ฿	1 x Buy now
Ammo, 50 Rounds	45 EUR = 0.219 ฿	1 x Buy now

Top dark web websites 2021

- DuckDuckGo. DuckDuckGo is the most popular private search engine. ...
- The Hidden Wiki. The Hidden Wiki is a good way to start accessing the dark web. ...
- Daniel. Daniel is another excellent way to explore the dark web. ...
- ProPublica. ...
- Sci-Hub. ...
- Hidden Answers. ...
- SearX. ...
- 8. Facebook onion site.