***7******Reading*: The difference between the Deep Web and the Dark**

**Web**

🕮 **Read the following article and answer the questions below.**

The dark web and the deep web are often used interchangeably, but they’re two distinct concepts. The common perception is that both are hotbeds of criminal activity including things like child trafficking, drugs, and contract killing.

The deep web is the part of the internet that’s inaccessible to search engines like Google and Bing. Think of the deep web as any content hidden behind some kind of access control such as a log-in or code word. Also referred to as “non-indexed” content, the deep web is several times larger than the searchable, or “surface,” web.

While the deep web can be a refuge for criminal activity, some folks might want to set up websites that aren’t meant for public viewing and, therefore, shouldn’t come up in search results. Your Gmail inbox, for instance, is also part of the deep web because it doesn’t exist as a publicly accessed domain.

A few other examples include online forms, WordPress staging links, and some academic journals. Such websites exist in directories that Google (and other search engines) are barred from crawling.

At the moment, search engines index north of 4 billion webpages. While that seems like a lot, it’s a mere fraction of the amount of information on the deep web. [According to some estimates](https://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104), the deep web is about 550 times larger than the surface web.

The dark web, also referred to as the darknet, is sometimes considered to be a small subset of the deep web. However, unlike the deep web, the dark web is as indexable as the clearnet, and search engines for the dark web exist, too. Some of these are [Candle](https://gjobqjj7wyczbqie.onion/), [Not Evil](https://hss3uro2hsxfogfq.onion/), and [SearX](https://ulrn6sryqaifefld.onion/" \t "_blank).

Much like the internet itself, the dark web is the product of the U.S. government attempting to build communication networks for military and self-defense purposes.

The Tor browser, used to access darknets, was designed to facilitate anonymous message sharing among U.S. spies spread across the world. Tor’s development began in the ’90s, and it was released as publicly available software in the early 2000s.

While the original aim of the dark web was to facilitate secret communication, the network’s anonymous nature also encouraged illegal activity. Helped by the launch of Bitcoin in 2009, the dark web quickly became a platform for criminals to source and deliver illegal items.

All activity here is anonymous by default as the only way to access the dark web is through the encrypted Tor browser. Neither users nor web administrators reveal themselves to each other, including their identity or their location. Hence, it’s very hard to shut down dark web servers or place geo-restrictions on users.

The dark web is definitely where the murkiest transactions on the internet take place. A [study](https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085) by researchers at King’s College London that examined the contents of over 2,700 darknet sites found that approximately 60% of them hosted illicit content.

The Silk Road, perhaps one of the most well-known examples of an illegal marketplace in the darknet, was shut down in 2013 but not before it showed the world how easy it was to buy illegal drugs, counterfeit documents, and other questionable items online.

In fact, it can be argued that the closure of Silk Road and subsequent arrest and conviction of Ross Ulbricht, its founder, only heightened interest in darknets and their illegal wares. Sociologist Isak Ladegaard, who built an algorithm to monitor sales data on Silk Road-type marketplaces, [declared](https://www.wired.com/2017/05/silk-road-creators-life-sentence-actually-boosted-dark-web-drug-sales/)

that all the media coverage enhanced people’s awareness of the existence of the dark web. As a result, trading actually went up.

But the dark web isn’t only associated with illegal activity. Whistleblowers, journalists, and activists frequently log on to the dark web in order to stay anonymous and spread the results of their research. [WikiLeaks](https://wlupld3ptjvsgwqw.onion/wlupload.en.html), for example, hosts a site on the dark web. Even Facebook, DuckDuckGo have websites on the dark web.

The dark web and the deep web are often conflated. The easiest way to understand the difference is that not all deep web is the dark web but all dark web is the deep web.

The deep web is simply the part of the internet that cannot be accessed by search engines. It might be password-protected or exist solely on staging servers. Accessing the deep web doesn’t require a special browser or unique protocols.

The dark web, however, can only be accessed through the [Tor browser](https://www.torproject.org/download/). The encrypted nature of the browser means everyone trying to access the dark web remains anonymous by default. What’s more, URLs in the dark web are starkly different from regular web addresses.

All sites on the dark web end with “.onion,” as opposed to “.com” or “.org” commonly seen on the surface web. That’s a deliberate ploy so that only browsers with specific proxies are allowed to access those sites. It’s also very difficult to remember the URLs of [sites on the dark web](https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/), which is another way to maintain their anonymity.

While Tor is the most popular way of accessing dark nets, the Invisible Internet Project (I2P) is another decentralized anonymizing project that deploys similar principles to Tor. Effectively a self-contained internet, I2P allows users to send emails, write blogs, and chat anonymously much like they would on the regular web.

Using the Tor browser or trying to access a non-indexed page is perfectly legal. Just because a page cannot be accessed by search engines doesn’t mean it’s trying to promote illicit activity.

Similarly, logging on to the Tor browser in order to browse the dark web doesn’t mean you’re breaking any laws. What is illegal, however, is buying illegal items like drugs or counterfeit documents, regardless of what browser you use.

In fact, you must practice extreme caution when trying to navigate the dark web. Don’t click on random onion URLs and make sure you verify a site’s authenticity before logging on. The dark web is full of scams and hackers trying to steal your data through phishing. Some useful sources on Reddit to verify onion sites include /r/deepweb, /r/onions, and /r/Tor.

If you plan on accessing the dark web, we recommend that you do so [in combination with a VPN](https://www.expressvpn.com/vpn-service/tor-vpn) to add an additional layer of encryption and anonymity. What’s more, use a burner email address, encrypt your messages with PGP, and disable Javascript on your Tor browser.

The government and your internet service provider can’t track your activity on the Tor browser, but they will know that you’re on the Tor network. That might attract attention, so you need to practice extreme caution to maintain anonymity.

1. How is the deep web distinct from the surface web?
2. What are the reasons for the deep web to exist?
3. What made it possible for the dark web to flourish?
4. What boosted illegal trading?
5. Are all activities on the dark web deemed to be illegal?
6. What are the differences between the dark web and the deep web?
7. How can the dark web be browsed safely?