**What is Dark Web-**

### **The dark web is part of the internet that isn't visible to search engines and requires the use of an anonymizing browser called Tor to be accessed.**

The dark web is a part of the internet that isn't indexed by search engines. You've no doubt heard talk of the “dark web” as a hotbed of criminal activity

The dark web is a subset of the deep web that is intentionally hidden, requiring a specific browser—Tor—to access, as explained below. No one really knows the size of the dark web, but most estimates put it at around 5% of the total internet. Again, not all the dark web is used for illicit purposes despite its ominous-sounding name.

The dark web is an area of the internet that is only accessible with specific browser software, such as Tor or I2P. It is a web of anonymity where users’ identities and locations are protected by encryption technology that routes user data through many servers across the globe – making it extremely difficult to track users.

The anonymity of the dark web makes it an attractive technology for illegal purposes. Unfortunately, gaining visibility into criminal locations is difficult: it requires specialized knowledge, access to closed sources, and technology that’s capable of monitoring these sources for misuses of your data.

**However, let’s first dispel some misconceptions about the dark web.**

1. **Assumption 1: The dark web is synonymous with the criminal internet.**While the dark web is home to lots of crime, it also hosts many legitimate companies like [*New York Times*](https://open.nytimes.com/https-open-nytimes-com-the-new-york-times-as-a-tor-onion-service-e0d0b67b7482) and [Facebook](https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648/) who offer Tor-based services, as well as generally benign content. The dark web is not synonymous with cybercrime.
2. **Assumption 2: The dark web is the same thing as the deep web**. To clarify, the deep web is broadly defined as anything that is not indexed by traditional search engines. Unsurprisingly, the deep web is also home to criminality – but so too is the clear web. The dark web does not monopolize cybercrime.

**Difference between deep web and dark web**

The portion of the Internet that is hidden from conventional search engines, as by encryption; the aggregate of unindexed websites is the deep web. And the dark web is the portion of the Internet that is intentionally hidden from search engines, uses masked IP addresses, and is accessible only with a special web browser: part of the deep web.” The key takeaway here is that the dark web is part of the deep web.

## What do the dark web and the deep web have in common?

What the *dark web* and the *deep web* have in common is that they are both hidden from commercial search engines. You cannot access either from Google or Bing. The *deep web* is a general, catch-all term that includes the *dark web*, but also includes “mundane content like registration-required web forums and dynamically-created pages like your Gmail account,” according to Andy Greenberg at [*Wired*](http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/). That is to say, most of the *deep web*is irrelevant to the news stories about Silk Road.

When people discuss the seedy underbelly of the Internet where you can buy drugs, weapons, child pornography, murders-for-hire—basically any illicit item or service you could dream up—that’s the *dark web*. Greenberg notes that while the *deep web* is vast and accounts for 90-something percent of the Internet, the *dark web* likely only accounts for about .01 percent. The*dark web*, sometimes referred to as *Darknet*, is accessed by Tor (The Onion Router) or I2P (Invisible Internet Project), which use masked IP addresses to maintain anonymity for users and site owners. This way, people who use the *dark web* for illegal purposes can’t be traced.

**Why dark web is dark –**

**The Structure of the Internet**

The internet is broken into three parts, the open, deep, and dark web. Most of us use the open web and deep web daily when we browse our favorite blogs and log into social media. However, the dark web’s content is not accessible through “traditional browsers or standard browsing technology” and is designed to be hidden from search engines, preventing them from appearing on the clear web.

**Browsing and Privacy**

Users are tracked across the clear and deep web via IP (Internet Protocol) address. With this information, website owners can ‘see’ users’ physical locations when accessing their site. IP also allows tracking services to record your website visits – selling this information to marketers who develop ads that “follow” you online. Dark web browsing technology negates these issues by anonymizing traffic. The encrypted routing technology at the core of the Tor Network, an example of dark web browsing technology, circumvents IP tracking and thus adds a layer of privacy for users online.

**The Takeaway:** The use of dark web browsing technology is not indicative of criminality. Users can and do utilize Tor and other tools to protect themselves on the clear and deep web too.

**Why Dark Web?**

As mentioned above, to access and browse the dark web, browsing technology, like the Tor network, is utilized. VPNs, Tor browsers, and even operating systems are leveraged to protect the user from being tracked and identified. Hundreds of communities exist on the dark web, from healthcare to politics, the dark web ecosystem hosts a diverse number of entirely legitimate and legal websites, organizations, e-commerce platforms, and social forum.

**Privacy Enables Criminality but Not on Purpose**

While the anonymity enjoyed by dark web users serves as a foundation for the thriving dark web fraud economy, the dark web also acts as a shield for persecuted groups, persons under oppressive regimes, and whistleblowers.

**The Takeaway:** The dark web, practically, is a privacy tool created to protect users’ identities while they traverse the internet for various reasons. Cybercriminals are leveraging the dark web to build hidden e-commerce platforms that specialize in the trade of your stolen data, counterfeit goods, and multiple services. These e-commerce platforms are powered by the demand for and availability of sensitive data.

### **Why surface web and dark web are not in a same platform?**

The main difference is that the Surface Web can be indexed, but the Deep Web cannot. You can still access it though. You yourself spend a lot of time in the Deep Web, but you probably do not know it. Deep web site examples are:

* Websites you can only get in with a username and password, like email and cloud service accounts, banking sites, and even subscription-based online media restricted by paywalls
* Companies’ internal networks and various databases
* Education and certain government-related pages
* Dynamic content, coming from a database where the page you see was displayed as a result of a query you put into that page's search box or a form (Crawlers can’t do these things.)

Note that bits and pieces of the data out of the Deep Web may be picked up by search engines in the case of a [data breach](https://blog.knowbe4.com/equifax-reports-data-breach-possibly-impacting-143-million-u.s.-consumers) or targeted attack.

### **And how is the Dark Web different from the Deep Web?**

At the moment, the Dark Web is defined as a layer of information and pages that you can only get access to through so-called "overlay networks", which run on top of the normal internet and obscure access. You need special software to access the Dark Web because a lot of it is encrypted, and most of the dark web pages are hosted anonymously.

There are several tools used for reaching these parts of the internet. The [TOR (The Onion Router)](https://www.torproject.org/index.html.en)maintains the most popular tool for Dark Web access. Their primary product is the [Tor browser](https://www.torproject.org/projects/torbrowser.html.en). If you think you are completely anonymous though, think again. Law enforcement routinely shuts down and prosecutes sites and people doing illegal things on the Dark Web.

On the Tor network, internet traffic is directed through the network of random relays. The browser builds a route of encrypted connections, one-by-one. Each relay knows only the previous and the next relays, but full connection route stays almost untraceable. The Multiple layers of encryption resemble the structure of an onion.

**How e-commerce works on dark web –**

The dark web has flourished thanks to [bitcoin](http://money.cnn.com/infographic/technology/what-is-bitcoin/), the crypto-currency that enables two parties to conduct a trusted transaction without knowing each other’s identity. “Bitcoin has been a major factor in the growth of the dark web, and the dark web has been a big factor in the growth of bitcoin,” says Tiquet.

Nearly all dark web commerce sites conduct transactions in bitcoin or some variant, but that doesn’t mean it’s safe to do business there. The inherent anonymity of the place attracts scammers and thieves, but what do you expect when buying guns or drugs is your objective?

Dark web commerce sites have the same features as any e-retail operation, including ratings/reviews, shopping carts and forums, but there are important differences. One is quality control. When both buyers and sellers are anonymous, the credibility of any ratings system is dubious. Ratings are easily manipulated, and even sellers with long track records have been known to suddenly disappear with their customers’ crypto-coins, only to set up shop later under a different alias.

Most e-commerce providers offer some kind of escrow service that keeps customer funds on hold until the product has been delivered. However, in the event of a dispute don’t expect service with a smile. It’s pretty much up to the buyer and the seller to duke it out. Every communication is encrypted, so even the simplest transaction requires a [PGP key](https://sela.io/pgp/).

Even completing a transaction is no guarantee that the goods will arrive. Many need to cross international borders, and customs officials are cracking down on suspicious packages. The dark web news site [Deep.Dot.Web](http://deepdot35wvmeyd5.onion/) teems with stories of buyers who have been arrested or jailed for attempted purchases.

In the day-to-day life of the regular law-abiding internet user, the dark web is mostly a scary unknown. Insofar as the average consumer knows, that side of the web – which is accessible only via a TOR server – is the place where their personal information is sold whenever there is a data breach.

A slightly more knowledgeable consumer might also know that the dark web is where one goes to buy illegal things with [**bitcoin**](https://www.pymnts.com/tag/bitcoin/).

And there is something to those particular stereotypes, since credit card numbers, passwords and Social Security numbers are all available for sale on the dark web. And, in the grand scale of [**illegal things up for purchase**](https://www.thetalko.com/15-messed-up-things-actually-being-sold-on-the-deep-web-black-market/), credit card numbers are pretty tame. For example, if one happens to be looking for weapons, hard legal or illegal drugs or [**uranium**](https://vocal.media/01/craziest-things-you-can-buy-on-the-dark-web), the dark web has all three up for grabs in various marketplaces.

Despite bitcoin’s reputation as the coin of the realm, when it comes to buying heavy narcotics, a bazooka or other such nefarious items, cash tends to be the preferred means of exchange. As it turns out, there are complaints galore from arms and drug dealers that [**bitcoin transactions are sketchy**](https://pirate.london/ive-been-scammed-for-my-bitcoin-buying-illegal-firearms-on-the-darknet-i-want-to-sue-4fa2ac1bcba3).

But perhaps the most surprising thing about the dark web isn’t how many horrible things you can buy there, but all of the genuinely weird transactions that occur. Some are illegal, but most actually aren’t – and they tell a slightly different story of the internet’s least understood, darkest corner of the web.

I**t’s A Matter of Trust, Kind Of**

Dark web marketplaces rely on “mutual anonymity and reputation.” Vendors encourage their customers to leave positive reviews, which in turn, give vendors “trust level” rankings, which, much like Amazon and Alibaba. Vendors with higher rankings capture more market share.

**Marketing and Community**

Dark web fraud vendors utilize fraud forums for a number of activities. Within these forums, fraud vendors promote their wares and services, while also interacting with prospects. These forums also serve fraudsters, those purchasing the stolen information. Fraudsters use forums to request specific goods, services, and sometimes seek partnerships to assist in fraud schemes.

## ****Inside look into the Dark Web e-Commerce Shopping Experience****

With all that stolen data floating around, hackers have transitioned from using it for themselves, and have begun to sell it to scammers online.

Since it is illegal to try and sell unauthorized data it is sold on the [Dark Web](http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-beautfiulpeople-3593569/). Besides special authorization and software to access, which allows users to interact anonymously via [Tor browser](https://www.torproject.org/projects/torbrowser.html.en), the overall experience is very similar to your traditional online shopping experience.

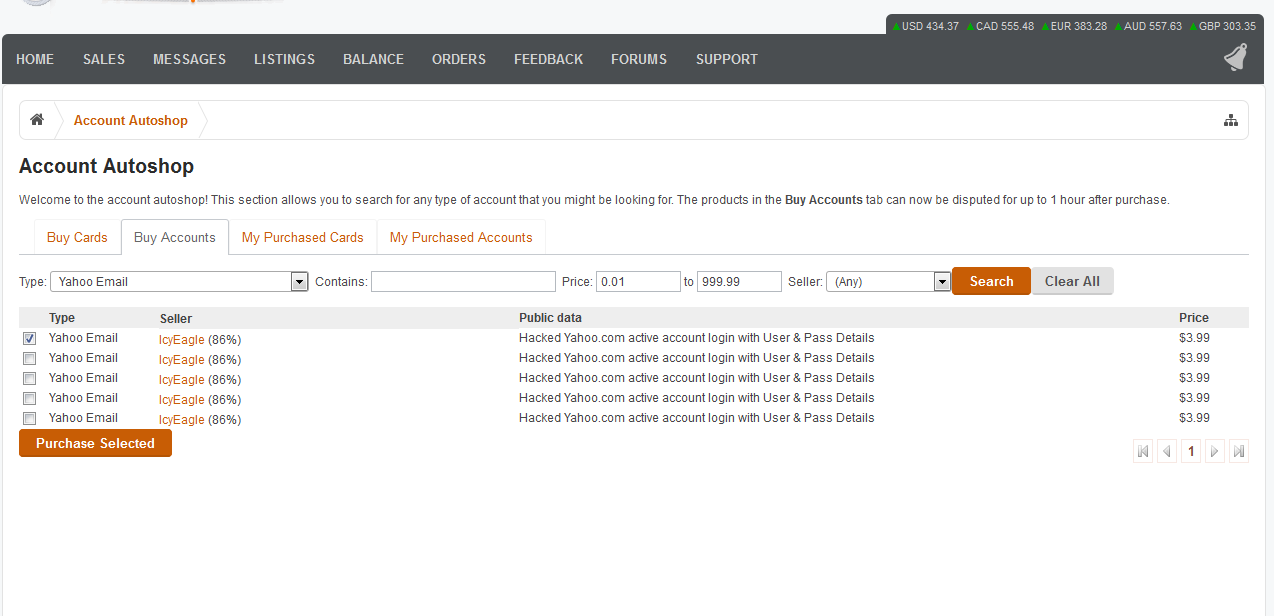
As Dark Web is becoming more sophisticated it is starting to adopt some of the principles of the traditional ecommerce retailers. They are offering “autoshop” experience coupled with anonymity. Some sellers even have refund policies!

In order to keep transactions anonymous the marketplace operates in [Bitcoin](http://www.coindesk.com/bitcoin-on-the-dark-web-the-facts/), an unmarked and untraceable digital currency, and they often sell their goods at prices cheaper than you’d expect and with the ease of immediate download or shipment.

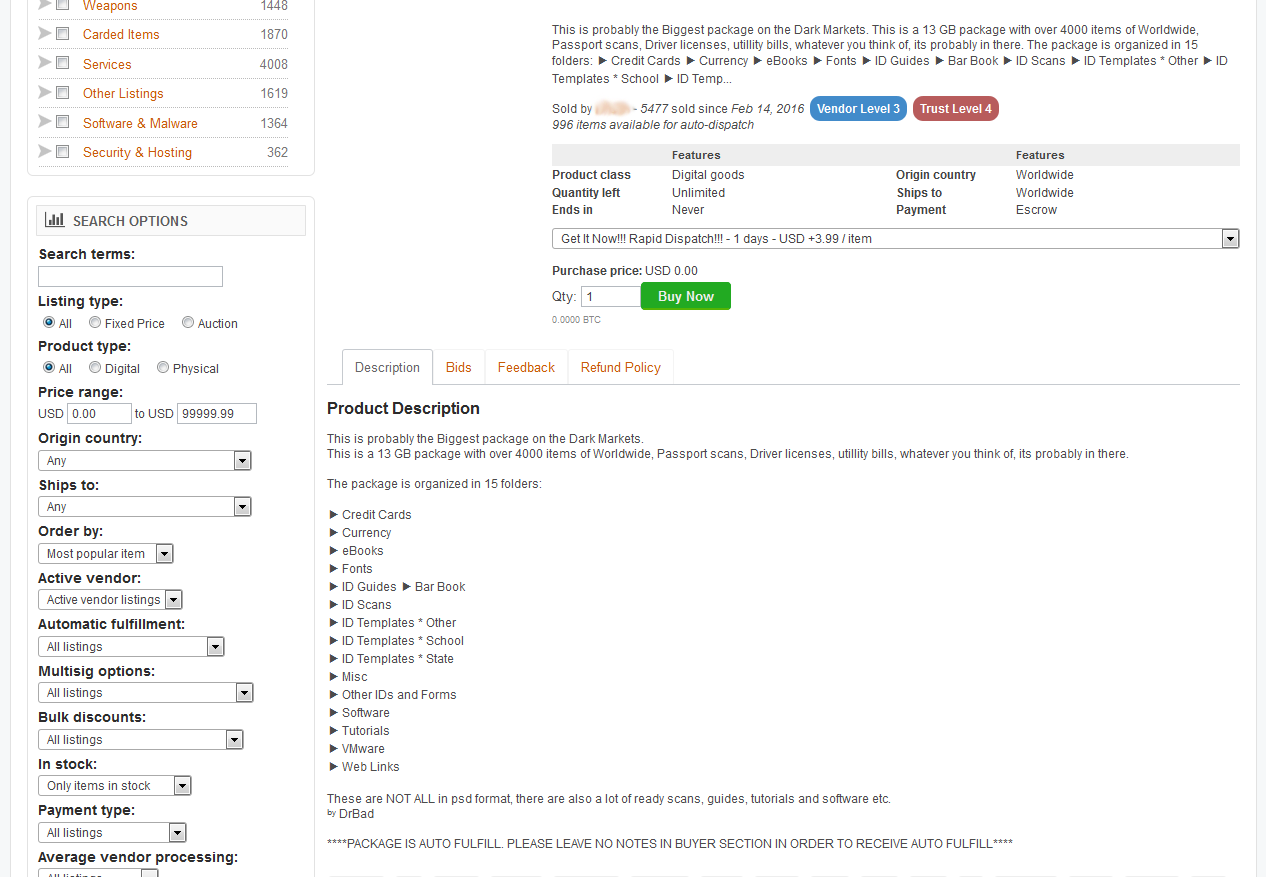
Platforms like these are so much more than just rudimentary command line setups or chat rooms. They offer many of the same features as online stores like Amazon or Ebay with vendor ratings, buyer feedback, detailed search options and facilitated transaction and delivery services. Collections of data are presented with detailed descriptions (similar to an ecommerce product pages), and some even provide tutorials on how to best utilize that data to scam victims.

Here is an example of the user-friendly design of one store found on the Dark Web, and how openly they shop the information of a yahoo user.

This is all too common in these marketplaces.



You can see just how easy it is for the Dark Web users to search for products by any number of qualities including category, product type, price, sale type, location and shipping options. The stores are designed to make shopping and buying as easy as possible for scammers and fraudsters.



## ****Ways to Keep Accounts Safe****

The boom in available personal information, the regularity with which is has been passed around, and the smooth auto shops on which it is sold, has created fast and easy ways for Hackers and scammers to access your information. This means it is easier than ever for scammers to steal your identity in order to access both private and professional information.

For businesses, this means you should take extra care to protect your information. It’s necessary to be vigilant in your security and develop [consistent monitoring habits](http://www.telegraph.co.uk/money/consumer-affairs/how-to-check-if-your-financial-data-is-for-sale-on-the-dark-web/). Here are some tips for keeping your information safe:

### **Change Your Passwords Regularly:**

* Changing passwords automatically makes much of what Hackers are selling unusable. The more often you change login information, the more positive you can be that no one is accessing your accounts.

### **Use Multiple, Complex Passwords:**

* Employees that use similar logins for their company and private accounts open up their employers to being hacked. Encourage them to use several passwords with numbers, capitals and symbols that are unrelated to information like birthdays or addresses.

### **Keep Track of the Activity on Your Accounts:**

* Many websites that hold personal information will alert you to unusual activity or logins to your accounts, but it is also important to keep an eye on it yourself, and make sure to investigate anything that appears out of the ordinary.

### **Monitor the Dark Web for Compromised Information:**

* While difficult, it can be done, particularly be people that are trained to do so. A professional service can not only inform you when your information has been compromised, they can advise you as to where you system’s weaknesses might be and help to prevent a breach all together.

The more you do, and the stronger your security is, the less likely it will be that Hackers will be able to collect your data and sell it online. The threat of compromised information is always out there, and with online marketplaces as prevalent and easy to use as they are today, the threat is only rising. Keeping you and your business’s information safe is more important now than ever before.

* **ABOUT VERICLOUDS**

VeriClouds was founded by [Rui Wang](https://www.linkedin.com/in/rui-wang-65b7729) and [Stan Bounev](https://www.linkedin.com/in/stanbounev) in 2014 to resolve the authentication security issues in Cloud Services. Information Security is not just a business opportunity. It is a calling, a passion, even an obsession. Rui and Stan joined forces to create ways to make the world more secure by making it safer to do business online. Rui has a Ph.D. in Cyber Security, and Stan is a successful entrepreneur with over 14 years of corporate and startup experience in the banking and technology industries.