How the Dark Web works

Beneath our everyday internet lurks a murky network of encrypted sites known as the Dark Web. Is it all bad? No. But it does fuel a lucrative criminal subculture that could threaten businesses and consumers.

The Dark Web is an ominous network of shadowy hackers hellbent on stealing company data, overthrowing the country, and selling drugs to your kids with Bitcoin.

Or is it? The hidden and encrypted internet enables hackers and activists and criminals. It's also a wonderful source for shocking headlines and [salacious YouTube stories](https://www.youtube.com/results?search_query=Dark+Web), and a communication and privacy-enhancing platform. Powered by a network of encrypted websites and accessible only by using a complex set of security tools, the Dark Web is as intriguing as it is beguiling. To understand the realities of the hidden internet, better grab a flashlight.

The Dark Web and the [deep web](https://en.wikipedia.org/wiki/Deep_web) are terms often confused and used interchangeably. The deep web is a term that refers to sites and pages unavailable to the general public and not indexed by traditional search engines, like corporate intranet sites, private social media posts, and pages with [nofollow](https://en.wikipedia.org/wiki/Nofollow" \t "_blank) search tags.

[Cybersecurity spotlight: The ransomware battle](http://www.techproresearch.com/downloads/cybersecurity-spotlight-the-ransomware-battle/) (Tech Pro Research)

Above the deep web hovers the [clearnet](https://en.wikipedia.org/wiki/Clearnet_(networking)) , the traditional internet and mobile web used by billions of people around the world. The clearnet is secure, and encryption is used to move secure data from place to place all the time. SSL guards passwords and protects credit card information during e-commerce transactions. But the very nature of the clear internet is that anonymity is rare. Computer and mobile IP addresses are constantly logged and easily traced. Cookies help web marketers track online activity and analyze behavior.

What differentiates the so-called [Dark Web](https://en.wikipedia.org/wiki/Dark_web) is the method by which sites are accessed. The Dark Web, or darknet, is a network of sites with encrypted content, accessible only with a secure suite of secure-browsing tools, like [Tor](https://www.torproject.org/). Tor -- an acronym for [the onion router](https://en.wikipedia.org/wiki/Tor_(anonymity_network))-- is a package of open-source security tools written for a customized version of the Mozilla Firefox browser, compatible with Windows, OS X, and Linux. The software encrypts user traffic and passes the IP address through the complex of Tor nodes.

These 'onion layers' help protect the user's anonymity and provide access to similarly protected websites. These sites range from forums to wiki pages to blogs and function much like clearnet sites. Dark Web domains frequently employ non-memorable, hashed URLs with the .onion top level domain. These sites block inbound traffic from all non-secure internet connections.

Personal and work computers often house mission-critical data, like sensitive files, passwords, and health records. Because Tor can be used and the Dark Web can be accessed on a traditional home PC, security professionals rely on additional security tools like the [Tails](https://tails.boum.org/) operating system. Tails is a Linux distribution that can be installed on and run from a portable flash drive. By accessing the Dark Web via Tails, user behavior is never logged locally, and it is significantly more challenging for malicious software to harm the host PC.

The Dark Web is used frequently by good actors for legitimate reasons. Encryption, security, and privacy are [championed](https://www.zdnet.com/article/the-impossible-war-on-encryption/) by news organizations, tech companies, universities, and activists in repressive regimes. The [U.S. State Department helps fund the Tor project](https://www.torproject.org/about/sponsors.html.en), and according to the [United Nations](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc), encryption is a [fundamental human right](http://www.techrepublic.com/article/why-citizens-need-encryption-as-a-fundamental-human-right/). Facebook operates a widely used secure Dark Web [portal](https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648) to the social network.

SEE: [Down the Deep Dark Web is a movie every technologist should watch](http://www.techrepublic.com/article/review-down-the-deep-dark-web-is-a-movie-every-technologist-should-watch/) (TechRepublic)

Yet it is also true that the Dark Web is an opaque, sometimes twisted, reflection of the clearnet. Crime is profligate. Black markets enable the morally libertine to profit handsomely in Bitcoin. The most famous Dark Web market, the [Silk Road](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)), allowed vendors and buyers to conduct business anonymously and enabled the sale of drugs, guns, humans, identities, credit card numbers, zero-day exploits, and malicious software. The site was raided and shut down by the FBI in 2013, but the idea of an anonymous, encrypted black market spread rapidly. Today, the site [Deep Dot Web lists dozens of Dark Web markets](https://www.deepdotweb.com/dark-net-market-comparison-chart/).

[](http://www.techrepublic.com/resource-library/whitepapers/special-report-cyberwar-and-the-future-of-cybersecurity-free-ebook/)

[Special report: Cyberwar and future of cybersecurity](http://www.techrepublic.com/resource-library/whitepapers/special-report-cyberwar-and-the-future-of-cybersecurity-free-ebook/)

You can download our full special report as a PDF in magazine format. It's free to registered ZDNet and TechRepublic members.

[Read More](http://www.techrepublic.com/resource-library/whitepapers/special-report-cyberwar-and-the-future-of-cybersecurity-free-ebook/)

"The Dark Web operates a lot like the clear web," said Emily Wilson, Director of Analysis at security firm[Terbium Labs](https://terbiumlabs.com/). "The same crime that happens off line, all the time, also happens on the Dark Web." In many ways, she said, because it's relatively easy to visit Dark Web markets, it's sometimes easier to see criminal activity as it happens.

Although it's not necessary for the layperson to visit the Dark Web often, if ever, every consumer is at risk of identity theft and should have a basic understanding of how the encrypted internet functions. Businesses should be aware that data from hacked companies and the government is easy to find and purchase on the encrypted internet. [A number of companies](http://www.techrepublic.com/article/four-misleading-myths-about-the-dark-web/), including Tripwire, ID Agent, and Massive, monitor the Dark Web and help businesses respond to Dark Web data leaks.

The Dark Web is not entirely malicious, but it's also not a safe place to visit. Novices and experts alike should exercise care and caution when visiting the Dark Web. ZDNet does not condone illegal or unethical activity. Offensive material can sometimes be just a click away. Browse at your own risk. Never break the law. Use the Dark Web safely, and for legal purposes only.

SEE: [Network Security Policy](http://www.techproresearch.com/downloads/network-security-policy/) (Tech Pro Research report)

The Dark Web -- like encryption -- is a double-edged sword. The hidden internet enables both good and bad actors to work uninhibited anonymously. And like encryption, the Dark Web is a reality for both consumers and business. Companies need to know about the Dark Web, Wilson said, and they need to be prepared for incidents to occur.

But consumers and companies shouldn't overreact to perceived threats. The Dark Web is not enormous. "Compared to the clearnet, the Dark Web is maybe a few thousand, or few hundred thousand [sites.]," Wilson explained. "Only a few thousand return useful content, and compared to the clearnet there's tiny amount of regular Tor users."

----------------------------------------------------------------------------------------------------------------------------------

# Is the dark web illegal?



*Written by Dan Rafter for NortonLifeLock*

*This article is intended to provide general, educational information and is not legal advice.*

There's plenty to see on the web, everything from the scores of your favorite sports teams to weather reports, reviews of the new French restaurant in town, and gossip from your friends and family members on social media platforms. But there's another world on the web that's mostly hidden from view and requires special browsers to access: the dark web.

If that name sounds sinister, it's because the dark web encourages activity that people would rather hide from view. The dark web is where people can buy illegal drugs and firearms. It's also dotted with sites that specialize in illicit pornography, including child pornography. It’s a part of the internet that you can’t find with traditional search engines such as Google.

Because it is hidden, [getting to the dark web](https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html) isn't easy. Most visitors first download Tor, or The Onion Router, a browser that allows users to search the internet anonymously. You can download this browser at [torproject.org](https://www.torproject.org/).

Finding specific sites on the dark web isn't easy, though. You have to know what you want. You can visit [thehiddenwiki.org](https://thehiddenwiki.org/) to see a list of dark web sites. Be careful when browsing that list, though. There are plenty of illegal sites on it.

The dark web was created, then, for people interested in surfing the internet anonymously, and the sites within the dark web often cater to illegal activity.

But are you breaking the law just by visiting the dark web?

## The dark web itself: Illegal or not?

The simple answer? The dark web itself is not illegal\*. What’s illegal is some of the activity that occurs on the dark web. There are sites, for instance, that sell illegal drugs and others that allow you buy firearms illegally. There are also sites that distribute child pornography.

The dark web itself, though, is not illegal. It offers plenty of sites that, while often objectionable, violate no laws. You can find, for instance, forums, blogs, and social media sites that cover a host of topics such as politics and sports which are not illegal.

## Is it illegal to access and browse the dark web?

Using Tor to access and browse the dark web is not illegal\*. You will, though, have to be cautious. Surfing the dark web might not be illegal. But visiting certain sites, or making certain purchases, through the dark web is illegal.

If you use the dark web to purchase illegal drugs or firearms, that’s illegal. You won’t be committing criminal acts, though, if you use the dark web to participate in forums or to read hidden blog posts anonymously. There are exceptions. You could potentially be participating in illegal behavior if you participate in certain forums, especially if it includes threats, hate speech, or inciting or encouraging criminal behavior.

The key here is to use common sense. If something is illegal outside of the dark web, it will be illegal in this hidden section of the internet, too.

## How much illegal activity is there on the dark web?

Looking for something illegal on the dark web? You’ll find plenty of options. In 2015, Daniel Moore and Thomas Rid, researchers at King's College in London, studied 2,723 sites on the dark web during a five-week period. The researchers said 57 percent of those sites hosted illicit material.

Of course, 2015 is a long time ago. The amount of illegal activity on the dark web has continued to grow. A University of Surrey 2019 study found the number of harmful dark web listings increased 20 percent since 2016. That accounted for 60 percent of all listings.

If you search the dark web, for instance, you’ll find online marketplaces that sell everything from Netflix passwords to stolen credit card account numbers. You’ll find other sites where you can buy illegal software, prepaid debit cards, and hackers for hire.

One of the better-known illegal sites on the dark web was Silk Road, an online trading site that sold fake IDs, heroin, and other illegal materials, that became a booming, if illicit, business after its founding in 2011. The site's operator, using the pseudonym Dread Pirate Roberts, became a sort of folk hero of the dark web, offering online surfers the chance to buy illegal goods anonymously using bitcoin.

The FBI, though, shut down Silk Road in late 2013. The agency also arrested Ross Ulbricht, the real person behind the Dread Pirate Roberts fake name. Ulbricht is now serving life in prison without the possibility of parole.

Two more recent examples of thriving criminal enterprises on the dark web were AlphaBay and Hansa. The FBI, U.S. Drug Enforcement Agency and the Dutch National Police, along with Europol, shut down these online marketplaces in the summer of 2017. According to Europol, AlphaBay and Hansa were responsible for the trading of more than 350,000 illegal commodities.

The marketplaces sold illegal drugs, firearms and malware. AlphaBay hosted more than 250,000 online listings for illegal drugs and more than 100,000 listings for stolen IDs, malware, firearms and counterfeit goods. Europol estimated that $1 billion of sales were made through AlphaBay since its founding in 2014.

Hansa wasn't quite so busy but ranked as the third-largest marketplace on the dark web as of its takedown in 2017, according to law-enforcement agencies.

It’s important to remember, though, that the dark web isn’t used solely for criminal activities. There’s a dark web version of Facebook, for instance, that people can use if they live in a country that censors social media. Reporters might use the dark web, too, to communicate with sources who want to protect their identities from hostile governments.

## Is it safe to access and browse the dark web?

If you’re careful, you can safely access and browse the dark web. First, download the Tor browser, which will give you access to dark web sites and keep you anonymous while searching the sometimes-seedier corners of the internet.

Tor will allow you to visit websites that have the .onion extension. That’s why Tor’s full name is The Onion Router.

You might consider investing in a [VPN](https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html), or virtual private network, too, when accessing and searching the dark web. A VPN helps keeps you anonymous when searching the internet, whether you are scanning the surface web or the dark web. When using a VPN, most likely only you and your VPN provider will know what sites you have visited. While it is legal to use a VPN in the U.S., it is always the user’s responsibility to familiarize themselves with other countries’ laws before using a VPN outside the U.S.

## I found my personal information on the dark web. What should I do?

What if you find your own credit card, bank account, or other personal information on the dark web? What if you find sites selling your Social Security number or checking account number online?

Unfortunately, there’ s not much you can do to remove your information from the dark web once it’s there. You should, of course, change the passwords you use to access your banking and credit card accounts. You might also want to update your login credentials to any services you subscribe to (like Amazon Prime, Netflix, or a meal delivery service, for example) and your healthcare and insurance accounts.

You might also consider placing [a credit freeze](https://www.lifelock.com/learn-credit-finance-credit-freeze.html) with each of the national credit bureaus, Experian, Equifax, and TransUnion. When you enable a credit freeze — which is free — you restrict access to your credit report which means lenders won’t be able to pull your credit. This can help prevent thieves from opening new credit cards or taking out loans in your name.

A credit freeze, though, cannot stop all criminal activity. If identity thieves have gained access to your credit card account, for instance, they can still use your card to make fraudulent purchases.

You should also order your credit reports from Experian, Equifax, and TransUnion. You are entitled to one free copy of each of your three reports once a year. You can order your reports from [AnnualCreditReport.com](https://www.annualcreditreport.com/index.action).

Once you do, study these reports for anything unfamiliar or unusual. If your reports list a credit card account under your name that you don’t remember opening, that might be a sign that thieves have used your personal information to sign up for a card in your name. Call that credit card provider and tell them that you never opened the account.

If you suspect that you have been the [victim of identity theft](https://www.lifelock.com/learn-identity-theft-resources-help-protect-yourself-identity-theft.html), file a report with the Federal Trade Commission [here](https://www.identitytheft.gov/). Next, contact the companies at which the fraud occurred — usually your bank or credit card providers. Inform each of the three major credit bureaus, too.

Finally, consider investing in a credit-monitoring service that can alert you whenever potentially suspicious activity occurs on one of your financial accounts. This type of monitoring could help you catch identity theft before extensive damage is done.

You might consider signing up for [Norton 360 with Lifelock](https://www.lifelock.com/#planschart), which provides identity theft protection, device security, and online privacy — all of which can be helpful in protecting your information from being accessed.