What Is the Dark Web?

by Ellen Sirull, August 22, 2017, Experian.com

You may have heard the term "dark web," but it can sometimes be difficult to understand what it really is and what it can mean to you. It may help to look at the internet as made up of different levels based on the access available and common purposes. There are three levels—the publicly available world wide web, the deep web and the dark web—and we'll explain a bit more here about each:

World Wide Web

This area is open to the public and includes anything you can find in a Google search:

- Blog posts
- YouTube videos
- Corporate and Personal websites
- Social Media

The public web is the Internet you surf, search and enjoy today—and it includes our website. Although most of our internet activity takes place on the World Wide Web, it comprises only 4% of all the content on the internet.

Deep Web

More than 90% of the information on the internet is in the deep web—a private area that is not accessible by search engines. The deep web is not malicious, however. It simply contains areas that are password-protected and unavailable to the public. Deep web components include:

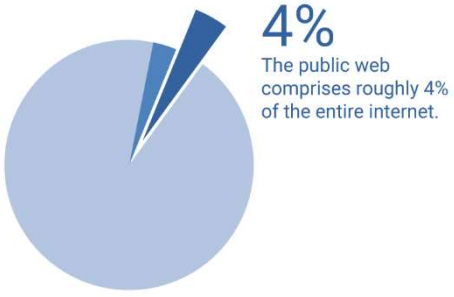
- Your personal bank account
- Retail accounts
- Member-only sites
- Internal school or company websites

These sites aren't anything to be concerned about—they're just one layer removed from the public web that's searchable through search engines.

Dark Web

The dark web is a hidden layer of the internet that is not accessible or indexed by search engines, and that requires specific software for access. This area is popular with criminals because they can remain anonymous and untraceable as they communicate. The dark web is where stolen information, such as bank account numbers and SSNs, is sold—often many times.

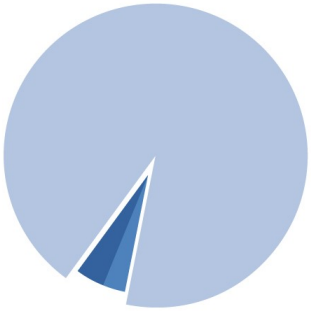
The Public Web



If you're like most people, this is where you spend the majority of your time—doing things like online shopping, searching for information and sharing photos and videos on social media. However, this represents only about 4% of the internet. While this isn't where identity thieves spend most of their time, there are things you can do to protect yourself online and keep your personal information from getting into the wrong hands while you surf the web. (See also—How to Avoiding Phishing Scams).

The Deep Web

The deep web is the next level of the Internet, representing approximately 90% of what's actually online. These sites aren't indexed by search engines, meaning they won't show up in any search results. Just because information is here, it doesn't mean it's something bad or illegal, though.

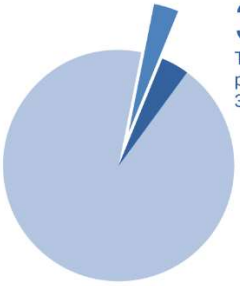


The deep web includes:

- Internal company sites
- School intranets
- Online databases
- Member-only websites or pages behind paywalls

These sites may live in this space because they're something that the owners don't want accessible to the public. Many deep web sites are legal, just purposely hidden. Sometimes you may hear the deep web referred to as a "bad" place to go, but that's usually because many people confuse the deep web with the dark web.

The Dark Web



At the bottom part of the deep web lies the dark web. The dark web isn't an actual place, but rather a hidden network of websites. While it requires special resources, it's just a matter of steps and getting certain systems set up that provide a way in for those looking to join the dark web and keep information such as their IP address hidden.

Visitors here utilize anonymity software to mask visitors' true identities. When you visit a website on the world wide web, IP addresses trace online activity on your computer. But on the dark web, with the masking software activated, a computer takes a randomized path to its file destination, bouncing around a number of encrypted connections to ultimately mask both location and identity.

Why Is the Dark Web So Popular with Criminals?

Because of its hidden nature and the using special applications to maintain anonymity, it's not surprising that the dark web can be a haven for all kinds of illicit activity (including the trafficking of stolen personal information captured through means such as data breaches or hacks). This means if you've ever been a victim of a data breach, it's a place where your sensitive information might live. According to the ITRC, data breaches in the United States during 2016 hit an all-time high of 1,093, which represents a 40% increase over the previous year.

Once exposed, this information that can change hands again and again over time—especially if it's a valuable combination of information (like medical information, a Social Security number, or an identifying address with account information) that's attractive to those looking to acquire stolen data. On the dark web, people looking for this information can get access to records that live online and are often available inexpensively—such as bundles going for less than $10 per record. These bundles are often called 'Fullz' because they include the full package for fraudsters: name, SSN, birth date, account numbers and other data that make them desirable since they're rich enough to do immediate damage. Savvy cyber-thieves also may wait some time before using the data they buy, because immediately following a breach, many people are more guarded and on the lookout for red flags on accounts, bills and their credit report.

Unfortunately, there are entire communities in the dark web and even sites the provide reviews on identity thieves that indicate if someone is "good to do business with" — meaning their data is valuable (think of it as the Yelp reviews for criminals). These criminals can make a decent living by selling, buying and using personal information.

How Can You Protect Yourself from the Dark Web?

People often aren't worried about the dark web until something like a data breach happens and they're notified their information was stolen. There's no fail-proof way to keep your information off the dark web because hackers are always trying the latest new thing to get your information and sell it to those looking to pay for it, but you can be vigilant about looking for red flags that your identity is in someone else's hands, including:

- Monitor your accounts and statements for any information that looks off
- Check your credit report regularly to see if inquiries or new accounts appear that you don't recognize
- Use strong passwords, and change them often
- Consider an online product to help you protect your identity and monitor your credit.
- Know how to respond immediately to suspicious activity

By staying on top of potential issues, you can help minimize the impact if your personal information does fall into the wrong hands.