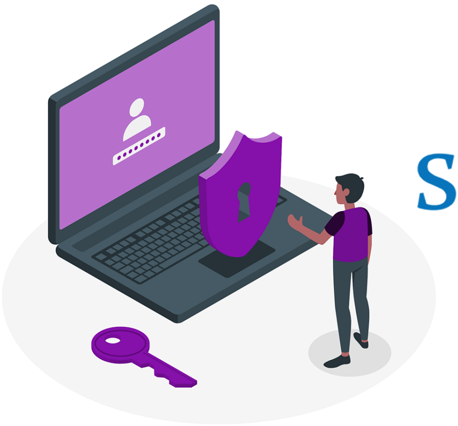

SECURUS ID

powered by experian

Understanding the Dark Web So You Can Keep Your Sensitive Information Safe

The dark web. Sounds frightening, right? Many of us have heard of the dark web but know very little about it. Let's take a few minutes to unpack dark web basics, why it's important to protect your sensitive data and how you can do this.

What is the dark web?

Often confused with the *deep web*, the dark web is a hidden part of the deep web that is estimated to make up about 5% of the total internet. The dark web uses encryption software that keeps users and their locations anonymous. Users must access the dark web through a browser called Tor.

Tor was created by the U.S. Naval Research Laboratory in the late 1990s to keep government communications private. Over the past couple of decades, however, the use of Tor and access to the dark web encompasses much more.

What is the dark web used for?

Because of its hidden nature, many illegal and nefarious activities take place in the dark web space. These activities include illegal drug and weapons sales, distribution of pornography including child pornography, solicitation and online gambling. The dark web is a popular place to purchase credit card numbers and counterfeit money, stolen subscriptions and hacker software, among other things.

However, not all dark web activity is illegal. In fact, the dark web has several legitimate uses. Here are some legal reasons people access the dark web:

- The dark web facilitates communication in countries where free speech is threatened and the government spies on its citizens.
- The dark web hosts online versions of out-of-print books.
- The dark web is a safe space for whistleblowers to expose corruption without fear of personal harm.
- Journalists often access the dark web when conducting research.
- Law enforcement agencies often access the dark web when conducting sting operations and investigations into illegal activity.

Threats on the dark web

The introduction of Bitcoin over a decade ago fueled dark web activity. Bitcoin allows users to conduct transactions 100% anonymously. Similarly, dark web activity fuels the demand for Bitcoin.

Bitcoin is the foundation of commerce on the dark web. Bitcoin is generally perceived as a secure form of payment. On the dark web, however, commerce is sketchy at best. Although there are plenty of commerce sites with shopping carts and customer reviews similar to those we're familiar with on the clear web, there are some major differences.

With a large number of shady characters running anonymous businesses on the dark web, sellers cannot be counted on to come through on their end of a sale or go to bat for you if you don't receive the item you purchased. Also, ratings and reviews can be easily manipulated to make an anonymous seller appear trustworthy when they're actually a scammer, out to steal your money...or your identity.

In addition to a shady e-commerce scene, the Into The Web of Profit report states several other threats on the dark web including but not limited to:

- Cyberattacks, including malware, DDoS and botnets
- Remote Access Trojans (RATs) and keyloggers
- Phishing
- Compromise of customer, operational and financial data
- Compromise of intellectual property, including trade secrets

End-user protection against exploitation on the dark web

If you visit the dark web for legitimate reasons, divulge as little personal information as necessary. Carefully guard your passwords, email and mailing address, account numbers and your SSN since all sensitive information can be distributed maliciously for financial gain.

Identity theft can happen anywhere online. One of your best defenses is an identity theft protection plan with Securus ID. See our plans here! Do you want to know if your personal information has already been compromised and is being distributed online? We would be happy to provide you with a complimentary dark web scan.