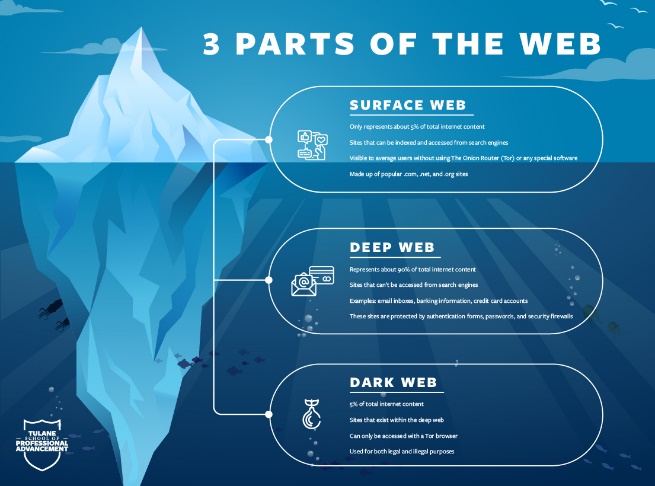
**1.Dark Web Overview**

The internet is a huge network of connections with a massive amount of information, however a large majority of it is not always readily available and is located on the Dark web. The Dark web is a is similar to the internet we all know and use, but is not accessible through normal search engines like Google. Certain software is needed to access the Dark Web as a large amount of illicit exists in this network. This illicit activity is almost always a threat to cybersecurity in some way.

The Dark Web is purposely concealed by search engines because of what exists in these networks. Many things can exist on the dark web but we will stick to cybersecurity related information for this article. Everything on the Dark web is generally concealed so you can’t track any locations or identities of any of the users. Most of the cyber related threats on the dark web consist of selling stolen data. This can be usernames and password combinations, information on a company, or new exploits.



**2. Why is the Dark Web a Security Concern for Cybersecurity?**

The Dark Web is a refuge hideout for cybercriminals whose goal is to remain anonymous and while carrying out their everyday unlawful activity. The Dark Web is the perfect place for this as it offers the anonymity and encryption that they want. On top of this, it acts as a marketplace for everything that they want to buy or sell. For example, login information can go for a hefty price on the Dark Web depending on how recently it was obtained, how easily, what company, and what permissions that account may have. They also can buy and sell credit card details, social security numbers, and day-zero exploits. All of this combined in a place can make it a huge threat for cybersecurity workers.

Prosecuting the people who are actively on these sites is extremely tall task as it is very difficult to track anyone on the dark web and almost anyone on this network is using untraceable currencies such as bitcoin to help hide their identity.

**3. How Can Organizations Protect Against Dark Web Threats?**

The best ways to protect yourself again the potential threats of the Dark Web is to take the necessary steps to secure your network and not give them a reason to have your data in the first place. Implementing security measures such as 2 factor authentication can help secure users account information, and having a cybersecurity analyst looking over a network for potential threats can help keep this at a minimum.

Educating your employees is one of the most important steps in reducing risk as phishing is one of the leading causes of information getting leaked. If employees know what to look for and which links are safe to click, then the companies overall risk will be decreased significantly from usernames and passwords getting leaked.

“Everything You Should Know about the Dark Web.” *Tulane School of Professional Advancement*, 29 June 2021, https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web.

The State of Cybersecurity By Darren Guccione, and Darren Guccione. “What Is the Dark Web? How to Access It and What You'll Find.” *CSO Online*, CSO, 1 July 2021, https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html.