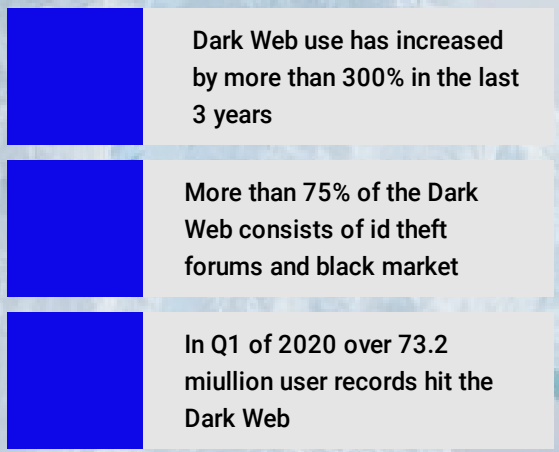
Infradapt
Outsourced IT for Businesses

Cyber Security, The Dark Web, & Your Charter

Did You Know?

The Dark Web is a hub for illegal activity where cyber criminals go to buy and sell stolen credentials. In fact:



- Dark Web use has increased by more than 300% in the last 3 years
- More than 75% of the Dark Web consists of id theft forums and black market
- In Q1 of 2020 over 73.2 miullion user records hit the Dark Web

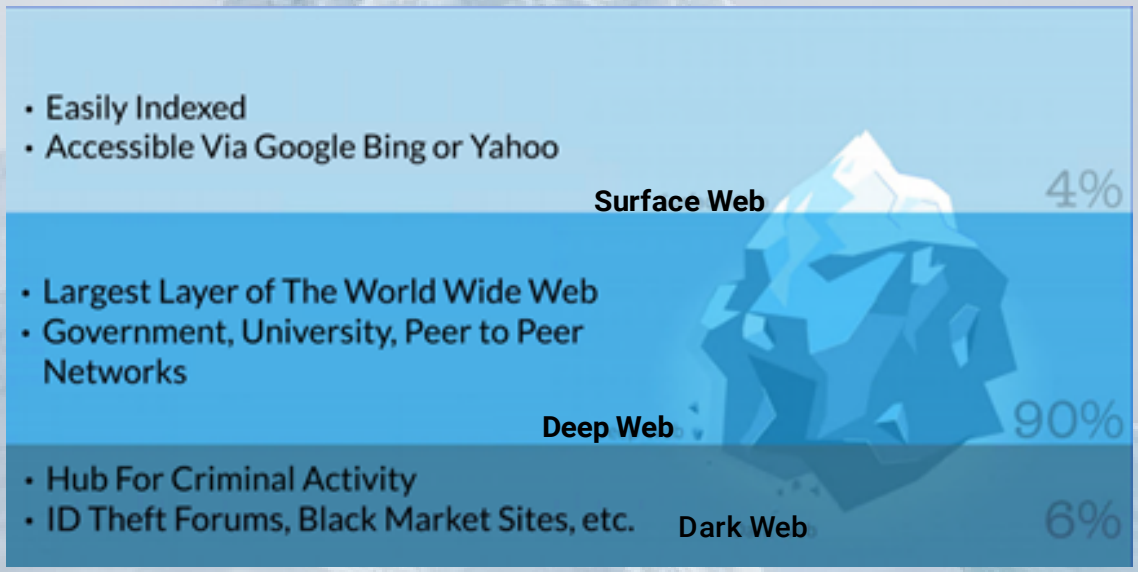
The World Wide Web:

The World Wide Web, at its core, is the very fabric through which we conduct business in today's society. From sending emails to handling sensitive data on a daily basis, the modern companies leverage web enabled tools to service their communities. That being said, the World Wide Web is just as expansive and intricate as it sounds – with many corners often unexplored by the average user.

The best way to imagine the structure of this virtual environment is to picture an iceberg floating in the ocean. There are 3 main parts to understand:

- **The Surface Web:** At the tip of the iceberg, above the water, is the surface web. This is what typical people use to access the common search engines like Google, Bing or Yahoo, along with any easily indexed site across the web. Surprisingly enough, the Surface Web only accounts for 4% of the sites on the internet.
- **The Deep Web**: Right below the tip of the "World Wide Web" iceberg, is the largest component of its structure, the Deep Web. The Deep web is the layer most commonly used for government networks, university research groups, and private peer to peer networks.

- **The Dark Web:** · At the very bottom of the iceberg, lies the Dark Web, or the portion of the internet most commonly used by cyber threat actors for a multitude of criminal activity. Being the final 6% of the internet, the sites on this area of the web are not easily indexed, and often times become the breeding ground for data breaches via id theft forums and dark marketplaces.



Academic Sector Under Attack

The numbers tell all: the academic sector has seen a 48% spike in ransomware attacks throughout the back to school season of 2020-2021. With the rise in remote learning, the attack surface of charter networks have increased, putting a major strain on the preexisting infrastructure and cyber security protocols in place. This has left countless administrations vulnerable to the evolving cyber threats skillfully crafted by hacktivists, rogue nation states, and for-profit cyber criminals. For this reason, it is important to be sure that Charter Schools shore up their defenses in the face of unprecedented cyber security risk.

There Is No Silver Bullet

There is no silver bullet to ensuring that your network will never get breached. While you can invest in the right infrastructure, implement the proper configurations, and keep up to date on the latest and greatest technologies, the biggest threat to any network will always be the end users – you, your team members, and your students!

Infradapt
Outsourced IT for Businesses

Right around 98% of all data breaches require an aspect of social engineering at some point in the process. Whether its convincing an financial administrator that money must be wired to a fraudulent account, or sending an email that tricks a user to click on malicious links, these messages are often times carefully targeted and routinely successful at manipulating their way in. With that in mind, the number one action that all administrators should take is to comprehensively train your staff in proper cyber hygiene, and maintain a sense of proactive awareness around your organizations overall cyber security posture.

Complimentaray Dark Web Study

50% of organizations have had a data breach caused by third party information theft. To do our part in the community, we are happy to provide any charter administrators with a complimentary dark web study to detect if any credentials related to their organization's domain has been compromised or put at risk.

For your free analysis, simply email chartertech@infradapt.com and use the subject line "Dark Web Study", and we will reply with a full report on anything we are able to find!

Additional Resources For PCPCS Members

Infradapt is committed to the professional development of public sector administrators regarding IT best practice. Guided by industry leading organizations such as NIST, CompTIA, CompTIA ISAO, SANS, etc., our team constantly keeps abreast of breaking news, evolving cyber threats, and best practices to engage the public sector community in meaningful ways.

Below is a link to a cyber security training seminar session that Infradapt conducted this December in partnership with PCPCS that goes more in depth on the cyber security "Who What, Where, & Why" that every administrator should know.

Webinar & Resource Link: Infradapt.com/chartertech

We also encourage administrators to maintain a dialogue with us by emailing chartertech@infradapt.com to be included on any breaking news, special offers, and Cyber Secure articles that we release throughout the year.