Cyber Security: What is the Dark Web?

By Jacob Goodson

You have probably heard the phrase “the Dark Web.” It sounds like a complex, sticky web of nefarious people conducting unethical activities—a place where legitimate businesses (like yours) should never enter. But what is the Dark Web, and how does it impact your company?

In its simplest terms, the Dark Web is part of the internet that is only accessible using a special web browser (such as Tor) that allows users and website operators to remain anonymous or untraceable. Accessing the Dark Web is not difficult. You can download Tor or another browser and be on the Dark Web within minutes.

An estimated 96% of the internet is not indexed by search engines; Google only crawls about 4% of the internet called the Surface Web. The other 96% is either Deep Web or Dark Web, and a lot of this is legitimate. The Deep Web includes things like medical records, financial data, legal documents, academic studies, company records, and other things that are behind firewalls or otherwise protected. But where the Deep Web is generally a place of privacy, the Dark Web is a place of anonymity.

Who uses the Dark Web? Anyone who wants to remain anonymous. This includes people who need to share information without risking their identities, such as journalists, informants, or whistle blowers. The Dark Web is also a notorious marketplace where you can buy all kinds of illegal things, kind of like Amazon for criminals.

At this point, you may be thinking, “this is interesting information, but my company doesn’t buy or sell illegal goods, so what does this have to do with me?” As we discussed in last week’s article on phishing, hackers are targeting organizations to gain access to money and data. The Dark Web is often the marketplace where they go to sell the data.

Now that you know what the Dark Web is, consider these business implications to Dark Web activities.

How do criminals use Dark Web data?
When information, such as user names and passwords, are available on the Dark Web, hackers can purchase the data and use it to access your network. Three common access points are your users’ email accounts, employee self-service, and VPN connections. Once inside your network, they have the ability to steal more data, cause further damage, and ultimately, cost your business more money to recover.

What does Dark Web monitoring do?
Dark Web monitoring scans for certain domain names or other criteria (such as pncpa.com) and lets you know if there is activity. It also monitors risky sites—places where people may be buying and selling “confidential” data. Again, back to last week’s phishing article, more than 60% of breaches take months to

discover. One way they are discovered is that the information is found on the Dark Web. It is an indicator that there is an issue, and allows a company to investigate and mitigate damage.

What benefit does Dark Web monitoring have?
By the time information surfaces on the Dark Web, the account has long been compromised, and multiple people probably have access to it. However, just because your domain is on the Dark Web does not mean that your network has been hacked. Many people use their business email addresses for non-business activities (such as LinkedIn). Whether your network has been hacked or not, you can use the information to help you reduce risks in the future. For example, you can make policy changes that prohibit employees from using their work email for non-work activities. You can also force password changes, either systematically or manually.

There are a lot of tactics you can use to strengthen your cyber security protocol with the information gathered from Dark Web scanning. Remember that while having your company's data on the Dark Web is an indicator of compromise, it's not necessarily a catastrophe. Using a reputable company to provide Dark Web monitoring services is one tool in your cyber security toolbox, but your provider should also be able to help you discern what to do with the information.