**Suggested Title: How Does the Dark Web Impact Small Businesses?**



Identity theft is an unfortunate occurrence that is all too familiar with most business owners, but do those individuals know where the compromised data will end up? Often, these business owners are unaware of the virtual marketplace where stolen data is purchased and sold by cybercriminals; a place known as the “Dark Web”.  An [article on Lexology](https://www.lexology.com/library/detail.aspx?g=9333b3f5-e404-479c-8d85-8c8491f318c9) explores what the Dark Web is, what information is available for purchase there and how it impacts small businesses.

**What is the Dark Web?**

The Dark Web, which is not accessible through traditional search engines is often associated with a place used for illegal criminal activity. While cybercriminals tend to use the Dark Web as a place to buy and sell stolen information, there are also sites within it that do not engage in criminal activity. For many, the most appealing aspect of the Dark Web is its anonymity.

**What is for sale on the Dark Web?**

Information sold on the Dark Web varies, and includes items such as stolen credit cards, stolen account information from financial institutions, forged real-estate documents, stolen credentials and compromised medical records. Even more alarming, the Dark Web contains subcategories allowing a criminal to search for a specific brand of credit card as well a specific location associated with that card. Not only can these criminals find individual stolen items on the Dark Web, but in some cases, entire “wallets” of compromised information are available for purchase, containing items such as a driver’s license, social security number, birth certificate and credit card information.

**What is stolen personal information used for?**

When stolen information is obtained by criminals, it can be used for countless activities like securing credit, mortgages, loans and tax refunds. It is also possible that a criminal could create a “synthetic identity” using stolen information and combining it with fictitious information, thus creating a new, difficult to discover identity.

**Why are stolen credentials so valuable?**

Stolen user names and passwords are becoming increasing popular among cybercriminals, but why? Identity thieves will often hire “account checkers” who take stolen credentials and attempt to break into various accounts across the web using those user names and passwords. The idea here is that many individuals have poor password practices and are using the same user name and password across various accounts, including business account such as banking and eCommerce. If the “account checker” is successful, the identity thief suddenly has access to multiple accounts, in some cases allowing them the opportunity to open additional accounts across financial and business-horizons.

**Why should small businesses be concerned about the Dark Web?**

Since the Dark Web is a marketplace for stolen data, most personal information stolen from small businesses will end up there, creating major cause for concern. With the media so often publicizing large- scale corporate data breaches, small businesses often think they are not a target for cybercriminals, however that is not the case. Cybercriminals are far less concerned about the size of a business than they are with how vulnerable their target is. Small businesses often lack resources to effectively mitigate the risks of a cyberattack, making them a prime target for identity theft as well as other cybercrime.

At a recent Federal Trade Commission (FTC) conference, privacy specialists noted that information available for purchase on the Dark Web was up to twenty times more likely to come from a company who suffered a data breach that was not reported to the media. The FTC also announced at the conference that the majority of breaches investigated by the U.S. Secret Service involved small businesses rather than large corporations.

**How can you reduce the risk for your small business?**

To reduce the risks of a cybercriminal gaining access to your company’s information/network, you must ensure you have proper security measures in place. The FTC has a [webpage](https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business) that can assist with security options for businesses of any size.  In addition, it is crucial that your employees are properly trained on security, including appropriate password practices. There is also talk of a government-led cyberthreat sharing program which would help enhance security across all industries by sharing cyberthreat data.