Dark Web Monitoring for Law Firms: Is It Worthwhile?

by Sharon D. Nelson, Esq., John W. Simek, and Michael C. Maschke

Most lawyers have no idea that the Internet is made up of several different areas, some of which are extremely difficult to access. When they use a browser to search for information or purchase products, they generally are accessing what is called the surface web. It is the information that is freely available with little or no restriction and accessible via search engines such as Google.

However, most internet information resides in what we call the deep web. Essentially, anything accessed using a password is considered the deep web. Examples would be email, bank accounts, medical records, etc. Think of the deep web as the portion of an iceberg that is below the surface and is not indexed by the search engines. Some reports put the amount of deep web data at 97% or more of the total internet.

Before we jump into the subject of dark web monitoring, let's discuss the dark web to set the stage.

Dark web access

The dark web typically contains sites that are associated with illegal activities such as child pornography, fraudulent services, drug trade, trafficking, etc. It is a minor portion of the deep web. Like other areas of the deep web, the content is not indexed and accessible via search engines.

Websites have .onion at the end of the site URL. The site address is a collection of scrambled text that isn't even close to identifying the site itself. As an example, the dark web URL for the CIA is http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/. At least it starts with ciadotgov.

Special software is used to access sites on the dark web. The Tor (The Onion Router) browser is most often used to access dark web data. Lawyers are always curious about the dark web and what evidence may be available there for their cases.

In fact, they often see the dark web as a "sexy" place to explore and want us to tell them how to safely access it. And yes it can be "sexy" in all kinds of ways, but our recommendation to attorneys is clear: **Don't access it.** Even if you have the technical knowledge to install and configure the Tor browser, securely accessing the dark web is simply beyond the skill level of most attorneys. In other words, to reverse Nike's slogan…Just Don't Do It!

Privacy

People hear the term "dark web" and immediately visions of criminal activity come to mind. Sex, drugs, guns, cyberattacks, etc. However . . . by its very design, the dark web is an excellent place to protect privacy. Journalists use the dark web to send and receive messages anonymously and to protect the identity of news sources. The dark web is also used to access information in countries where internet access is restricted. So it is not all evil, though much of it is – and it is best avoided as a destination.

Dark web marketplace

Unfortunately, the dark web is mainly used for illegal activity, as noted above. It is also a repository for stolen personal information that is typically put up for sale by cybercriminals. We will concentrate on marketplaces used to sell personal information such as stolen credit cards, bank account logins, medical records (yes, medical records are quite valuable in relation to other records) and other items where financial gain is the motive. It is the fear of personal information being disclosed on the dark web that has spurred such great interest in monitoring services. That is particularly true for lawyers who are ethically mandated to protect client confidential data.

Dark web information

A key question is "How did my personal data get on the dark web?" While each person's situation is unique, here are the ways cyber criminals gain access to your information. A common method is to have your computing device(s) infected with malicious software designed to capture your activity by stealing your passwords and user IDs.

Phishing scams are another method to get you to divulge your private information. You may end up on a malicious web page where you freely enter the requested information which is then transmitted to the cybercriminal. Another popular phishing scam gets you to call a phone number (typically toll free) to get technical assistance with a pop-up warning or to dispute a purported credit card charge for a service or item you did not purchase.

Commonly, your data ends up on the dark web because of a data breach. In other words, your information is held by another party (like a law firm!) and the firm suffers the breach. Since the pandemic, ransomware attacks have significantly increased. Many ransomware attackers exfiltrate the target's data first and then take various steps to entice the target to pay the ransom. Commonly, the exfiltrated data includes client information which may end up on the dark web.

Monitoring services

You may have seen commercial advertisements for services that monitor for identity theft. Services tend to start at around $100/year. The services promise to monitor various aspects of your life and alert you to suspicious activity. Basically, they monitor your credit score, as well as online and financial activity. Dark web monitoring is typically part of the service too.

How do they monitor and what does it mean to you? **Let us first say that we are not big fans of any of the monitoring services.** You will probably end up giving them all sorts of personal information so that they know what to look for and act on your behalf. They can't scan for release of your social security number if they don't know what it is. They'll need to know your credit card numbers to scan the dark web to see if they are available for sale. You get our drift.

Do you trust the monitoring company to have robust security in place to protect all the personal data you have entrusted to them? It seems to us that a monitoring service is very similar to a law firm in that it provides a "one-stop shop" for cybercriminals.

What about dark web scans? Frankly, we think many security and monitoring companies use dark web scans as the FUD (Fear, Uncertainty & Doubt) factor to scare you into paying them money. We see hundreds of dollars a month being charged to law firms just for dark web scans. The vendors will produce a report showing that your email address, social security number, password, etc. were found on the dark web. So what? The discovered data is usually stale (several years old) and of very little value. You've probably already changed your password for the discovered sites and implemented MFA too.

Get real value for your money!

One real value for a dark web scan is awareness. You should be able to obtain an initial dark web scan free of charge – without paying an ongoing monthly monitoring fee, which we certainly don't recommend. The initial report will help identify if you have law firm employees that tend to reuse the same password across multiple sites. It may even identify sites you were not aware of so that you can immediately change the password. Use the dark web scan to educate employees at your next cybersecurity awareness training session. If you're not teaching your employees about cybersecurity, at least annually, you are missing a very significant part of cyber resilience! A human element is involved in data breaches 82% of the time.

Take control of your data and don't hand it over to a monitoring service. You should be using a password manager and a unique password for each website or application you use. Put a freeze on your credit file at the three major credit bureaus. Freezing your credit file is free. Why would you want to pay someone to monitor your credit score since freezing your credit file will stop a huge amount of identity theft opportunities? A lot of credit cards offer free credit score reports too.

Final Words

If fear seems to be the driving force to get you to sign up for dark web monitoring, and it usually does, use the advice above and stop throwing your money away!

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.*

Michael C. Maschke *is the CEO/Director of Cybersecurity and Digital Forensics of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional. mmaschke@senseient.com.*