Why hackers target law firms

When hackers seek to access private information, they are generally looking to access as much valuable data as possible in the shortest amount of time… and what better place to find volumes of secure information than a law firm? While cybersecurity concerns have been around for many years now, it seems that incidents involving law offices are happening more often than ever before.

In the spring of 2016, more than 40 of America's top law firms were targeted for information on global mergers and acquisitions in one single hacking event. As reported by DataBreaches.net, the American Bar Association confirmed that approximately 25% of all U.S. law firms with 100 or more lawyers had experienced a data breach in 2015. These incidents occurred in the form of website attacks and break-ins. Lost or stolen items, like computers or cell phones also contributed to these statistics. During the same year, 15% of all law firms reported an unauthorized intrusion into the computer files of their practices.

It's a mistake to assume that only large firms face this risk. In June of 2016, a small Texas firm was the target of a hack into their email accounts. A fraudulent email was sent out from the firm's account. It targeted people across the U.S., Canada, and the United Kingdom. The email included an attachment with malware that infected computer systems and accessed financial records. Though the firm disabled the email account and posted a warning on its website upon learning of the breach, the personal information for thousands of people may have been compromised.

Why your firm is a target

Here are three reasons why hackers target law firms:

1. Hackers see an opportunity to take advantage of large quantities of valuable and quality documents. By targeting law firms, they can quickly access such information as technical secrets, business strategies, and financial data for numerous clients.
2. Law firms provide a quick detour around information of little value. Large corporations tend to store large amounts of data in their computer systems. However, the information they provide to outside counsel is usually more selective and valuable to hackers. By skipping the corporation and targeting your law firm, they more easily access the high-value data.
3. Law firms are notorious for having low levels of data security in place… even worse than the clients they are serving. The hustle and bustle of a law firm sometimes prevents owners and administrators from taking the time to upgrade security measures. But that doesn't have to be a problem.

TimeSolv legal billing software protects your firm data with state-of-the-art hosting services. We know that reliability is important to your practice, so we consistently strive for 100% uptime. With TimeSolv, you get the type of security that is constantly evaluating and responding to new and ever-changing threats, so your firm does not become a story on the nightly news.

About Erika Winston:

Erika Winston is a freelance writer with a passion for law. Through her business, The Legal Writing Studio, she helps legal professionals deliver effective written messages. Erika is a regular contributor to TimeSolv and a variety of other publications.