LEGAL
workspace
Your Law Office in the Cloud

Everything Your Need to Know About

Cryptolocker & Ransomware

Learn how to identify and prevent online threats targeting law firms.

A Legal Workspace® White Paper

Cryptolocker Strikes

Buzzzzzzzz-That's the sound of your alarm clock going off at 5AM, you have a big day ahead of you. You grab your phone, which moonlights as your alarm clock (among other things), and silence the alarm. With your phone in hand, you glance at your email — low and behold, there is the email from your client you've been waiting for! Quickly, your feet hit the floor, you move swiftly to your Keurig machine and brew up your morning cup while simultaneously powering on your laptop… Multitasking before 6am was not your plan, but you are very anxious to get logged in so you can open the attachment your client sent you.

Java in hand, shaking the sleep out of your eyes, you open your email, double click on that attachment you received, and you wait for it to open…. wait, why isn't it opening? You double click it again and still nothing. Hmm, maybe the third time is the charm… double click and nothing. Frustrated, you decide to check the news and browse the web while you wait for your file to open. You open your browser and POW! What's that noise? All of the sudden your computer is screaming at you and there is a message on your screen you have never seen before. Your computer is telling you it's been infected with a virus meaning all of your files are locked and encrypted. To regain access to your files you need to call a strange international number and provide them with 5000 bitcoins (not dollars, yen, or pesos, but bitcoins– Bitcoins. What's a bitcoin? Where do I get them?). Why is this happening to me? What on earth is going on?

What Is CryptoLocker and Ransomware?

You've just fallen victim to one of the most emerging cyber-attacks on the planet. The email you thought was from your client was really a "spoofed" email address from a fraudster looking to make a quick buck off the innocent and unsuspecting professional. In technical terms, it's called ransomware. The good news is, the story painted above did not actually happen to you, but it could.

Once considered a consumer problem, ransomware has morphed to target entire networks of computers at law firms and other businesses. These entities have more to lose than the average consumer making them prime targets for cybercrimes. According to the U.S. Department of Justice, ransomware attacks have QUADRUPLED this year compared to just one year ago, averaging about 4,000 a day. Typical ransomware payments range from $500 to $1,000, according to cyber-risk data firm Cyence Inc., but some hackers have demanded as much as $30,000. Every infection is unique and equally as painful to recover from.

How do you Prevent Cryptolocker and other Ransomware Attacks?

Now, you have to be wondering what you can do to prevent this happening to you and your entire practice….. The last thing you want to do is tell your largest client that all their matter files are corrupted, infected, and useless. The best thing you can do to prevent cyber-attacks from happening to you is to invest in your technology, know what you're up against, and train your employees. We recommend starting with the basics:

- **Anti-Virus Software:** You have a myriad of choices when it comes to Anti-Virus software. Companies such as McAfee, Trend, and Symantec offer suitable small business products. These can help catch the majority of these infections before they begin.

- **Look before you click:** When you receive an email with an attachment, look at the sender's address to make sure it's coming from their actual email address. Some spoofing attacks will use an email address that's very similar to a legit one – chris@gmaiil.com instead of chris@gmail.com. It's easy to overlook the extra letter in the domain name. If you question the email's validity, check with the sender to ensure they sent it. If it came from someone you don't know, or looks phishy (pun intended), delete the email immediately.

- **Augment your IT infrastructure to an IT Company**: Spend your valuable time practicing law not figuring out IT. Companies, like Legal Workspace, spend the time, money, and effort to implement enterprise-level protection against online attacks. You're in business to practice law, not understand and implement corporate IT solutions. Leave that to the experts.

I'm sure you're glad this situation did not happen to you, and so are we. The cyber world is moving at a vigorous pace that can be hard to keep up with. Employ legal technology professionals to keep up with emerging threats and cover your bases for you. Practice law, not technology — leave your cybersecurity worries to us.

Legal Workspace is a pioneer in cloud-based work environments and data storage designed specifically for law firms. Learn more at legal-workspace.com.