The ABCs of Malware.

A Law Firm's Guide to Understanding, Preventing, and Budgeting for Online Attacks.

PACE TECHNICAL

Table of contents.

PACE TECHNICAL

Viruses aren't the only thing you need to worry about.

Every day, hackers invent new ways to wreak havoc for personal gain.

You regularly update your antivirus software and everyone working in your office is trained to treat emails with suspicion and to avoid unsecured Wi-Fi networks; that should be all it takes to protect your office from a cyberattack...right? That may be more than what most firms are doing, but it's not nearly enough to keep you safe.

From front-page attacks like ransomware to less obvious "grayware," there are several types of malicious software programs and each one requires a unique defensive strategy. This is especially true for law firms, which according to Verizon's 2018 Data Breach Investigations Report, **account for 58% of cyberattack victims.**

At PACE Technical, we believe avoiding malware is just as feasible for small and medium sized firms as it is for enterprise sized firms.

You don't need a computer science degree to follow some basic cybersecurity best practices, and you don't need to hire a full-time technician with a six-figure salary to enjoy enterprise-level security. By the end of this eBook, you'll have a fundamental understanding of how hackers target law firms with malware and how to stop them from succeeding. Let's get started.

5 telltale signs of malware infections (beyond sluggishness).

Noticing one of these red flags could save you thousands of dollars.

For decades, you've been trained to look for a virus when your computer performed more poorly than usual. But as new types of advanced malicious software are released, hackers have made it harder to notice when something is amiss. Here are some lesser known signs your computer has been infected:

1. **Your security software is mysteriously disabled.**
2. **Filenames have changed for no reason.**
3. **Unknown apps or browser toolbars have appeared.**
4. **An unrecognized webpage pops up when you open a new browser window.**
5. **Your email contacts are receiving strange messages from you.**

If you notice any of these signs, shut down your computer immediately and contact an IT professional about stopping the malware.

Now, if you subscribe to managed IT services, unlimited tech support is included in your service. But for law firms that still rely on the "call IT repairmen after something breaks" model, malware prevention is going to be especially important.

Tips for avoiding the most common malware attacks against law firms.

Insight from PACE Technical technicians, who spend 7 days a week in the trenches of IT security.

Full disclosure, the majority of cyberattacks are made possible by users who circumvent security software and hardware. "Phishing" (sometimes called social engineering) is when hackers disguise themselves as a trustworthy source, such as a bank employee, and ask for private information, such as a credit card expiration date.

So, the best way to avoid almost any type of malware is security awareness training. But beyond that, there are some more black-and-white solutions.

Trojans.

What are they?

Trojans are programs that seem benign to unsuspecting users, but hide their true purpose. They accounted for 41% of all infections in 2017 according to Comodo's Global Malware Report. In one example, the Google Play store recently expunged a fully functional barcode scanning app that was secretly forwarding sent and received text messages without the user's knowledge.

How to avoid trojans.

Since Trojans are disguised as seemingly harmless apps, a cautious mindset is your best form of defense. In other words, be careful when installing free software, even if it comes from a trusted source like the Google Play store. Forbidding employees from installing software that isn't approved by your IT department is a good place to start.

Tips for avoiding the most common malware attacks against law firms.

Viruses.

What are they?

Viruses were some of the first malicious programs ever created. When a file is opened that is infected with a virus, that virus can spread itself to other files and computers. Applications and documents that are infected can be altered, stolen, or destroyed. Viruses aren't as popular as they once were, but in 2017 they were detected in 190 countries, with **Canadian individuals and businesses being the most common targets.**

How to avoid Viruses.

Because viruses can't hide behind the guise of a useful program, they are usually distributed as documents attached to emails. In addition to regularly reminding your employees to be wary of attachments, you should have a high-end spam filter and email-based antimalware software, ideally with real-time alerts and monthly audits from IT.

Tips for avoiding the most common malware attacks against law firms.

Worms.

What are they?

Worms are malware that spread themselves without the need for any human action. They are standalone programs that exploit network security holes and, unlike viruses, don’t need to be opened or installed to work. They hog a surprising amount of computing resources as they spread from victim to victim, but worms are most dangerous when they’re programmed to deploy viruses, ransomware, and trojans along their journey.

How to avoid worms.

Because they spread via deeply rooted hardware and software vulnerabilities, the most important thing to do is install vendor-issued updates and patches for apps, operating systems, and firmware. To illustrate how crucial this is, let us examine a horrific real-world example. In April 2017, Microsoft issued a patch for the vulnerability that made the WannaCry attack possible before the ransomware was actually released. The malware was so immensely successful only because so many people failed to update Windows.

Tips for avoiding the most common malware attacks against law firms.

Ransomware.

What is it?

Ransomware is set apart by its use of extortion and encryption. When a computer or server is infected, all its files are rendered unreadable until victims pay hackers a fee to return everything to normal. Ransomware actually dates back to the early '90s, but has become exponentially more effective, with a **massive spike of reported incidents affecting Canadian organizations in 2017.**

How to avoid ransomware.

Because it is based on unbreakable encryption, there's usually no recovering from a ransomware attack unless you have robust and secure backups stored somewhere safe from the spread of infection. Many off-the-shelf antimalware programs contain so-called ransomware protections, but struggle to recognize never-before-seen threats. A DNS security solution will allow you to scan for and defend against potential ransomware and other malware attacks. Cloud-based backups are also inexpensive and ensure your data is always accessible regardless of the latest advancements in ransomware infections.

Tips for avoiding the most common malware attacks against law firms.

Grayware.

What is it?

Grayware programs don’t actively alter, steal, or destroy information, but still manage to cause problems. This type of malware slows down your computer, reveals your private information, and floods your computer with ads. In the summer of 2017, a grayware application was found on 250 million computers. All it did was change a web browser’s default search engine, but it could’ve granted remote access to the computers it was installed on.

How to avoid unwanted applications.

These applications often come installed on new computers or bundled in free software packages. Take the time to periodically factory-reset company-issued devices. Windows 10 includes a user-friendly “Refresh” feature that wipes everything from a computer except its documents and critical applications. Anyone should be able to wipe a mobile device, but an IT services provider can do it in a fraction of the time.

$375 Million worth of mistakes prove malware isn’t “fake news”.

Law firms make for lucrative targets.

Ontario law firms - $90,000+.

In December 2012, two Ontario law firms were duped out of huge sums of money due to fraudulent emails (or phishing scams). In one of the cases, a lawyer lost $90,000 because of a bogus cheque collection service. The second firm suffered a six-figure loss after a bookkeeper accessed the firm’s bank’s website on a computer that was already infected with the Trojan Banker Virus, a strain of malware designed to steal financial account login information.

British Columbia law firms – $200 to $2,000.

Since 2013, British Columbia law firms have suffered from a string of ransomware attacks that were distributed using phishing attacks. Legal staff who unwittingly downloaded these malicious programs were forced to pay between $200 to $2,000 to recover their encrypted files. In extreme cases, some law firms paid more than $10,000 for the ransom, which was a huge risk considering that there’s usually no guarantee that cybercriminals will stay true to their word.

Major Canadian firm – $425,000.

In 2017, an established Canadian firm paid hackers $425,000 in Bitcoin to release its systems held captive by ransomware. Reports found that the ransomware attack not only encrypted the firm’s primary databases but also it’s backup systems, leaving the company with “no choice but to pay.” Investigators believe that the firm’s executives fell for a spear-phishing attack containing ransomware-ridden PDFs disguised as invoices.

$375 Million worth of mistakes prove malware isn't "fake news".

DLA Piper – $374 million.

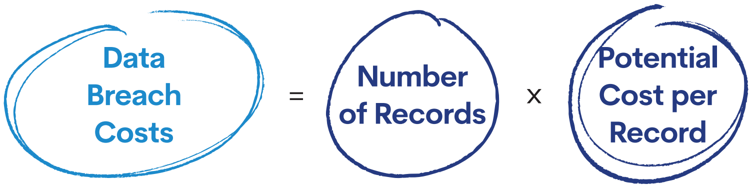
One of the world's largest law firms, DLA Piper, also fell victim to ransomware attack called Petya in 2017. Unlike common strains of ransomware, Petya was designed to destroy compromised files and make recovery impossible, which meant that the firm had to shut down their network to contain the infection and restore their systems.

Although DLA Piper didn't cut a deal with cybercriminals, the costs of the infection were severe. The entire firm's operations were completely halted, staff didn't have access to phones, emails, and legal documents for weeks, and there was significant damage to the firm's reputation. Overall, experts estimated that the damages totaled $374 million, all of which could have been avoided if the firm had installed Windows and network updates released earlier in the year. Undeniable proof that cybersecurity solutions are worth the investment

A formula for putting a dollar value on your security needs.

Undeniable proof that cybersecurity solutions are worth the investment.

Even without the information in this eBook, it's clear to most law firms that IT security services are non-negotiable. Budgeting how much to spend on those services isn't always as clear. Cybersecurity isn't something you want to skimp on, but we'll be the first to tell you that you shouldn't give an IT provider carte blanche. Thankfully, there's a simple formula to make sure the funds you set aside for prevention never exceed the costs of a breach:



Data Breach Costs = Number of Records x Potential Cost per Record

It's easy to calculate when you know the average data breach trends. For example, a 2018 Ponemon study estimates **that that the average data breach costs $81 (USD) per record**, So if your firm stores 5,000 records, you could be paying over $405,000 per breach.

Keep in mind that this is only the per-incident cost. Legal firms with subpar security measures and troves of legal records may experience data breaches twice a year — which we assure you is woefully optimistic.

24-hour malware protection doesn't have to cost an arm and a leg.

Prevention is much cheaper than reparation.

Knowing how to spot and avoid common types of malware can go a long way in protecting your business, but without around-the-clock security you'll never be totally safe.

We offer cutting-edge cybersecurity solutions designed to protect you against new and old malware threats. With our expertly configured antivirus software, firewalls, advanced intrusion prevention systems, data backup solutions, user training, and simulated attack testing, you'll never need to worry about the financial impact of a data breach again.

All our solutions are installed, configured, monitored, and centrally managed by a team of experienced professionals for less than the cost of a single in-house technician.

Managed IT.
Managed Better.

Want to see our approach to your cybersecurity firsthand?

Call us today to talk with one of our seasoned consultants.

We're happy to answer your questions, provide recommendations, and audit your current IT network.

Request your initial consultation today!
Phone: (905) 763-7896 Email: inquiries@pacetechnical.com

PACE
TECHNICAL