How Law Firms Can Prevent Phishing and Malware

Tuesday, February 4, 2020

Law firms harbor information directly linked to politics, public figures, intellectual property, and sensitive personal information. Because lawyers rely on email to manage cases and interact with clients, hackers exploit technical vulnerabilities and people via email. After cybercriminals infiltrate a law firm’s systems in a successful phishing or malware attack, they leverage breached information for financial gain.

Starting with email, law firms must control the availability, confidentiality, and integrity of data. Or they will suffer breaches that bring increased insurance premiums, loss of intellectual property, lost contract revenue, and reputational damage.

**Law firms aren’t securing their cloud technology**

As lawyers adapt with best practices in technology, they’re moving client data and confidential documents from on-premise to cloud-hosted databases. **58% of firms use cloud technology to manage their clients and run their firms**, according to the *2019 Legal Technology Survey Report* on Cybersecurity and Cloud Computing from The American Bar Association’s Legal Technology Resource Center.

Migrating data to the cloud is a good thing, despite concerns about its availability. Data is more secure when stored in a system with modern infrastructure and security protocols, instead of stored locally on an outdated system no longer supported by vendors — such as a desktop device still running Windows 7 software, rather than Windows 10.

Even though the cloud is safe, law firms inevitably fall victim to cloud-based cyberattacks like phishing and malware.

**26% of lawyers reported a security breach at their firm.** TECHREPORT’s other findings explain why the breach rate is so high:

- Fewer than half (41%) of all respondents changed their security practices after migrating to the cloud.
- Only 35% of lawyers adopt more than one standard security measure — like encryption, anti-malware, anti-phishing, and network security.
- 14% of respondents using cloud-based technology to manage their firm do not have any preventative security measures in place.
Lawyers know data breaches create downtime, loss of billable hours, and reputational harm. But they’re less aware of how to prevent those outcomes.

**Phishing explained**

Phishing happens via email, when hackers impersonate trusted senders to trick recipients into divulging sensitive or confidential information. Most often, phishers trick victims to click a malicious URL and interact with spoofed login pages. Microsoft is the most spoofed brand in the world, because it is the hub for organizations to collaborate and exchange information. If a lawyer enters their Office 365 credentials onto a spoofed login page, the username and password go directly to the hacker’s server.

Successful credential-harvesting phishing attacks allow hackers to access data-dense services like Office 365, online banking, and practice management software. Stolen credentials lead to account takeover scenarios that result in further exploits, including network infiltration, database infiltration, and data exfiltration.
3 common characteristics of phishing attacks

1. **Subject lines that appear highly urgent**

Many subject lines in phishing emails are in all-caps to pressure the recipient. Beware of subject lines that say “URGENT” or “Are you available?” An infographic from cybersecurity firm KnowBe4 reveals the top phishing email subject lines from 2019.
2. **Spelling errors, grammar errors, and awkward language**

Hackers need to deceive language parsing technology like Optical Character Recognition (OCR) that identifies suspicious content and blocks the message. To bypass anti-phishing algorithms, they'll intentionally misspell words, use special characters that look like letters, and replace letters with lookalike numbers. Phishing URLs are often misspelled, or the domain name does not match the content of the page. Carefully read every URL to see if the words and letters match the content of the page.

3. **Unexpected or unusual requests for documents or money.**
Phishers can spoof the sender name and domain of trusted contacts’ email addresses to lull recipients into a false sense of trust and compliance. Requests for sensitive information (bank routing numbers, trust account numbers, login credentials, document access, etc.) should be confirmed over the phone or any other communication channel besides that same email thread.

**6 ways to prevent phishing at your law firm**

1. **Check if email addresses associated with the firm were involved in high-profile breaches**

   Have I Been Pwned is a website that identifies compromised email addresses and passwords across online services that have been breached so that victims can change their password and prevent account access. Set up alerts through the website to monitor any future breaches.

   ![Have I Been Pwned](image)

   Source: [HaveIBeenPwned.com](https://haveibeenpwned.com)

2. **Install password managers**

   The best passwords don't need to be memorized. 25% of people reuse the same password for everything, according to OpenVPN. Password manager services like 1Password (paid) and LastPass (free) use browser plugins and mobile applications to create, remember, and autofill complex, randomly-generated passwords. They identify weak or reused passwords across websites, and run a program to simultaneously rewrite and save new passwords on those sites.

   ![LastPass](image)

   Source: [LastPass.com](https://lastpass.com)

3. **Make Multi-Factor authentication (MFA) mandatory at the firm**

   Multi-factor authentication, a secure login method using two or more pieces of confirmation, adds another step to
the login process to prevent account takeover and the breach of confidential data. When username and password credentials are submitted to the login page, MFA generates and sends a unique alphanumeric code to the account holder's email or phone for use as a secondary password. Unless this code is submitted on the follow-up login screen in a timely manner, it will expire.

Because email accounts and cell phone numbers are publicly available and can be compromised, use app-based and hardware-based MFA instead.

Solo and small/medium firms should use the Google Authenticator app, which continuously creates dynamic codes that swap out every 30 seconds and are unique to the device on which the app was installed.

Larger firms should adopt physical MFA. These “keys” plug into your laptop, tablet, or mobile device ports to authenticate access to software — and even the device itself. Because the keys are unique, hackers can’t access accounts supported by hardware MFA keys like Yubico’s YubiKey, which is used by every Google employee. If the key is lost, account access can be gained through backup codes or MFA codes delivered via email, mobile, or authentication apps.

4. **Participate in phishing awareness training programs**

These software programs regularly educate and train employees on the characteristics of spam, phishing, malware, ransomware, and social engineering attack methods. Microsoft’s Attack Simulator and KnowBe4 offer free programs that train users not to interact with phishing attempts and give visibility into how well they’re trained, based on their click rate during the attack simulations. The 2019 Verizon Data Breach Investigation Report found that lawyers and other professional service workers were the third most likely group to click on phishing emails.
5. **Only connect to secure WiFi**

Connecting to public WiFi in a cafe, airport, or hotel is dangerous. Malicious worms can transfer from one device to another if they are connected on the same network. When traveling, use a virtual private network (VPN) to extend a remote private network across the public network and secure the WiFi connection.

6. **Report suspicious emails**

Popular email clients like Office 365 and Google Gmail offer suspicious message reporting. Use this built-in tool to improve their anti-phishing algorithm. If applicable, contact the IT team or cybersecurity staff at the firm so they can update security configurations in the email client or third-party security tool they may use.

### What is malware?

Malware is any malicious file that launches scripts to hijack a device, steal confidential data, or launch a Distributed Denial of Service (DDoS) attack. Most malware is delivered via email. The 2019 Verizon Data Breach Investigation Report found that 51% of phishing attacks involve malware injections into a network. These malicious scripts are usually injected via spoofed DocuSign and Adobe attachments, or fraudulent billing and invoicing documents.

Ransomware is a subset of malware that hackers use to hold information or access hostage until a ransom is paid. Ransomware exploits frequently involve blackmailing tactics, and “sextortion” phishing emails (in which hackers purport to have footage of the victim watching pornography) are gaining popularity.

The 2019 ABA TECHREPORT noted that **36% of firms have had systems infected, and about a quarter (26%) of firms were unaware if they've been infected by malware.** Larger firms, which tend to use on-premise software because of the up-front work associated with cloud migration, are the least likely to know if they’ve suffered a malware attack.
3 ways to prevent malware

1. Monitor and update outdated software and hardware

Application updates are necessary and should not be treated as optional. These software upgrades implement essential security features to ward off new strains of attacks. Not updating software and hardware provides short term savings, but will be very costly in the long run.

Be aware that:

- Windows 7 is no longer supported since January 2020.
- MS Office 2010 will no longer be supported as of October 2020.
- Support for Adobe Acrobat X Reader/Standard/Pro, Adobe Acrobat XI, and Reader XI has ended. 88% of attorneys continue to use these highly-vulnerable Adobe programs, according to the 2019 ABA TECHREPORT.

2. Monitor email for links and executables (including macro-enabled Office docs)

Executable files automatically launch actions, based on the code in the file. Apply software restrictions on your device to prevent executable files from starting up without your consent. Microsoft found that 98% of Office-targeted threats use macros. In 2016, Microsoft pushed a macro-blocking feature in Word to prevent malware infection.

3. Hire a Managed Service Provider (MSP) for cybersecurity

MSPs offer an affordable portfolio of solutions to manage cyber risk across firm operations.

The solution: control the login process and data access in cloud-based apps

Lawyers are obligated to protect sensitive client information from phishing, malware, and ransomware. As breaches continue to make headlines, clients are selecting firms based on their data security. Law firms educated on confidentiality, security, and data control will be able to reassure security-conscious clients.

Cloud security — especially in email and document storage — relies on identity and access management. Establish a secure login process, govern user privileges in applications, and ensure that everyone at the firm can spot suspicious emails and attachments.

Choose cloud providers with a reputation for secure software and identify third-party security vendors for anti-phishing, anti-malware, and MFA.

Written by Reece Guida

© Copyright 2020 PracticePanther