LawPay®

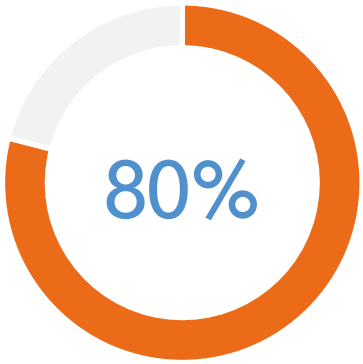
AN AFFINIPAY SOLUTION

# LAW FIRM GUIDE TO CYBERSECURITY

# Contents

# Introduction

Today's legal professionals know that data security is an urgent concern, now more than ever. Law firms are often in possession of their clients' most sensitive and personal details, so it is no surprise they have become prime hacking targets. "A majority of law firms have experienced some sort of hacking, with law firms that handle government contracts and international business being targeted most often," said Karin Conroy on Lawyerist.com. "About 80% of the largest 100 law firms have experienced some sort of violation."




"About 80% of the largest 100 law firms have experienced some sort of violation."
*-Lawyerist.com*

As such, it's wise to review all aspects of your data security strategies on a regular basis, including administrative practices, building protection, computer security, and information systems. But does this mean you have to immediately become an internet security expert if you want to avoid becoming the next headline or cautionary tale? Absolutely not! The following simple, manageable steps will help ensure better data protection in your practice and are easy enough that any firm can implement them.

CHAPTER ONE

# Identify Your Cyber-Assets

The path to a more secure firm starts with creating a simple document detailing your practice's IT assets. **Using our template**, list all of the technology you use at your firm, to the best of your knowledge. If you have an IT service or office manager, enlist their help to fill in any missing areas. There are four different categories you should explore when completing this template.

### Networking Infrastructure

Do you have wired (LAN) and Wi-Fi networks? What is connected to each? Is there a guest network? Who has access to the Wi-Fi passphrase(s)?

### Systems and Other Hardware

Take an inventory of all of the PCs, laptops, mobile devices, file servers, and network-attached storage (NAS) that are present in the practice.

### Applications and Data

What business software are you using, and what are those applications responsible for? Common software for law firms include practice management suites, billing and payments solutions, and document management tools. What information do they manage and where does that data reside (both cloud-based and on premises)? Don't forget about any backups and archives that you may have residing in different locations.

### Users

Make a comprehensive list of any and all users with accounts on your systems, including what privileges and capabilities these users have. For example, you might have administrative rights on your PC, but you may have created an account for your bookkeeper with access restricted to certain folders or files. Ask all members of your staff to help ensure this information is as complete as possible.

Creating a comprehensive inventory of all the assets in your practice is the only way for you to know exactly what items you'll need to protect. Once you have this information recorded, you have taken your first step toward making your law practice, and your clients' sensitive data, more secure.

CHAPTER TWO

# Strengthen Your Passwords

Everything in your office, from your network itself to your personal computer, is only as secure as the password you have created for it. Shockingly, security researchers have consistently found that a majority of people reuse the same password for many, if not most, of their applications. A single insecure website that exposes your password in a data breach could be all an attacker needs to gain access to many accounts that are critical to your practice and your personal life. So what steps can you take to protect your personal information and your firm's valuable data?

### Use a Password Manager

You can significantly strengthen your passwords by utilizing a trusted password manager application, such as 1Password or Keychain on Mac OS. A password manager provides a secure way to store and find all of your passwords, and only requires you to remember a single, master passphrase to gain access. Basic password managers work with a single computer, encrypting passwords on your hard drive. More sophisticated versions, however, allow you to share your passwords across multiple devices and computers, including mobile phones and tablets.

As you create new accounts for sites you visit or applications you use, add a new entry in your password manager. Name the entry after the site, include your username, and use the password manager to generate a password. Most generators will let you choose the length and complexity of the password to meet any rules imposed by the site, such as allowed special characters.

Some accounts may require you to provide answers to security questions to reset a forgotten password. Unfortunately, most sites ask the exact same questions and may not adequately protect the answers. If the account requires you to answer security questions, use the password manager to generate your responses, as well. Remember to include the security question in the password entry.

**Everything in your office, from your network itself to your personal computer, is only as secure as the password you have created for it.**


## Create a Strong Passphrase

When you first set up your password manager, you will need to choose a strong but memorable passphrase. A passphrase is basically a stronger, more complicated password. Strong passphrases have the following characteristics:

- Contain both upper and lowercase letters
- Have digits and punctuation symbols as well as letters
- Contain at least 12 or more letters, numbers, or symbols–the longer the better
- Are not a word in any language, slang, dialect, or jargon
- Are not based on any personal information, such as names of family members or pets, or important dates

## Enable Multi-Factor Authentication

Another step you can take to protect your critical systems is to enable multi-factor authentication–also known as MFA or two-factor authentication. Multi-factor authentication is available on many sites and protects you by requiring both your password and a code to access your account. The access code is typically texted to you or provided by an app on your phone, such as Google Authenticator, and changes with each use. Without access to both your phone and your password, an attacker is prevented from gaining access to your account.

In short, it is crucial to remember that your accounts are only as strong as the passwords you create for them. A trusted password manager is a great way to organize, secure, and diversify your passwords. Lastly, in cases where even stronger security is required for your systems, enable multi-factor authentication for added protection.

CHAPTER THREE

# Fortify Your Network

Wi-Fi networks make it easy to connect the systems in your practice, both to each other and the outside world. Unfortunately, they can also make it easy for an intruder to gain access to those same systems, and the data therein. The good news is that there are a few important, but simple, changes you can make to your network configuration to significantly reduce this risk.

## Secure Administrator Access

Start by using your password manager to set a strong password for administrative access to your wireless router. Many networks are breached because the default password was never changed. Log in to your router's configuration website to reset this password and update the other security options discussed in this tip. For most wireless routers, you access this website by entering "192.168.1.1" or "192.168.0.1" into your browser address bar. Note: To do this, you will need to make sure you are connected to your network first, either via an Ethernet cable or Wi-Fi.

With administrator access locked down, you should now secure access to the network itself. Most wireless routers today support a primary Wi-Fi network, one or more guest networks, and wired, local area network (LAN) ports to connect directly to the router. We recommend that you keep your office devices and staff on the primary Wi-Fi (your "private" Wi-Fi network) or LAN, and use a guest network for any clients or visitors who need internet access.

## Enforce Wi-Fi Authentication

Access to all of your Wi-Fi networks needs to be password-protected. For small businesses, the predominant standard is referred to as WPA2-PSK or WPA2-Personal, or just WPA2. WPA2-Enterprise can provide more flexible authentication options for larger practices with many users, but requires additional configuration that may require IT services. With WPA2-PSK, a shared password is used to access the network. Use your password manager to generate differing, strong passwords for both your private and guest Wi-Fi networks.

## Limit Guest Access

Your guest network is there to keep your clients and visitors separate from your private network—and out of reach of your confidential information. If you are not careful, however, you may inadvertently allow your guests much greater access. When configuring your guest network, you may see an option to allow guests to access your LAN, local network, or intranet. Make sure you do not allow LAN access so that your guests cannot reach office systems that are wired directly to the router.

## Configuring your Guest Network:

From your browser, find the wireless settings section of your router's configuration.

### For each wireless network:

1. Set a network name, or SSID.
   This is what users will see when they choose from available wireless networks. Clearly differentiate your private and guest network names.

2. Choose "WPA2-PSK" for the network authentication method and "AES" for the encryption method. Depending on your router, these may be grouped together or split into two separate options, and they may use different labels like "WPA2-Personal" or "WPA2." Don't use "WEP," "WPA" (without the 2), or "TKIP" (without "AES" included), as these options are less secure and may be easily circumvented.

3. Enter the password you generated for the network, also known as the pre-shared key.

### Keep Physical Security in Mind

Keep in mind that wireless routers can typically be reset to their factory configuration with just the push of a button or a straightened paper clip. Once reset, the default password is the only defense between an attacker and your network. If possible, keep your wireless router in a locked enclosure or cabinet with the reset mechanism inaccessible.

Your office's network is one of the most essential systems in your office, which is why protecting it is such an important security step.

CHAPTER FOUR

# Protect Your Internal Systems

As systems and processes become increasingly digital, computers are simultaneously becoming an increasingly attractive target for online attackers—providing a jumping-off point to access numerous systems and accounts. There are multiple routes into these systems, from open network connectivity to targeted malware—so let's explore some simple tools for protecting against these threats.

## Keep Your Systems Updated

One of the greatest threats to your internal systems is malware—software that is created specifically to damage or disable computers and their systems. Many malware threats operate and spread by taking advantage of problems in software for which fixes have long been enabled. Unfortunately, these fixes are often not applied to vulnerable systems. Modern operating systems such as Windows and Mac OS X support automatic installation of critical updates—you just need to enable it.

A number of application packages, such as Microsoft Office and Adobe Acrobat, also support automatic updates. Given their widespread use throughout business, these applications offer a rich target for hackers. If the applications you use offer automatic updates, make sure this feature is enabled.

## Install Anti-Malware Software

Clicking a link in email that looked legitimate, downloading a file from a site you thought was secure—these are all common actions taken every day that infect systems with malware, and the damage can range from keyloggers stealing passwords to ransomware holding your data hostage.

You can greatly reduce your risk of falling victim to these attacks by making sure antivirus or anti-malware software is installed and configured properly on all of your systems. Once installed, make sure real-time checking is enabled so that security analysis is performed immediately, as actions are performed. You should also schedule full computer scans weekly at a time that doesn't interfere with your work. If you are using Windows 8 or later, Windows Defender antivirus is pre-installed and needs only to be configured.

## Enable Your Firewall

A firewall inspects the communications coming in or out of your PC and determines whether to allow the communications to continue or block them. Firewalls can prevent attackers from gaining access to your computer and data, as well as halt the spread of malware from one computer to others. Windows and Mac OS X both have built-in firewalls that you can configure to meet the

needs of your office. You should enable your firewall and configure it to block all incoming connections except for applications that you specifically enable. Typical exceptions include instant messaging and file sharing applications. Some software applications may require specific exceptions to be configured to allow access from other computers on your network or the internet, but the vendor documentation should make this clear.

## Limit Access

One final recommendation for protecting your systems is to limit what users are able to access and modify. In computer security circles, this is known as the "Principle of Least Privilege" and states that users should have the minimum privileges necessary to do their jobs. By limiting users in this way, your confidential information is only accessible to specific individuals and non-administrative users can not make system changes that may threaten the security of your office.

We suggest creating an administrator user with full privileges to configure your PCs and individual, non-administrator accounts for each user in your office, including yourself (avoid using an administrator account for your primary account). Then, share files and folders with specific users based on their need to access information.

Any weakness in your system can expose a wealth of sensitive data to those looking to exploit it. Fortunately, by taking the steps above, you can help ensure your systems are significantly less vulnerable to hacks and data exfiltration from both within and outside of your office.

CHAPTER FIVE

# Secure Your Sensitive Data

The security and integrity of the data in your office is of paramount importance—especially considering law firms tend to have large amounts of confidential and sensitive information about their clients. In the course of accessing, using, and transferring this data, it can be found in a number of locations and forms. Not only are you ethically responsible for protecting this data, but in many cases, you are legally responsible as well. So what can you do to ensure sensitive data remains protected, regardless of its current state or location?

## Protecting Data in Motion

When handling sensitive information within a web browser, always make sure the address starts with "https," which indicates a secure connection. Data transmitted over a properly secured connection is encrypted and prevents an attacker from tampering with or accessing the information sent. Most browsers highlight the address bar in green or show a closed lock to indicate that the connection is secure.

Avoid using any website that your browser flags as having an untrusted certificate, as the site or connection may be compromised. For example, a browser might display a message stating "The site's security certificate is not trusted" or "There is a problem with this website's security certificate."

## Protecting Data at Rest

Data stored on your computer or a network storage device also needs to be secured. Most modern operating systems support "whole drive" or "whole disk" encryption. Once enabled, you can be comfortable knowing that if your computer is ever lost or stolen, the data stored on it cannot be accessed by anyone else.

To get started using whole drive encryption, search for "BitLocker" from the Start Menu on Windows Professional or "FileVault" on Mac OS X.

For data that is backed up off of your computer, or that needs to be transmitted to other parties, file encryption is a must. Applications like SecureZIP and OpenPGP implementations like Gpg4win (Windows) can be used to secure your own data for storage, as well as ensure protected communication to third parties.

**Beware of websites that may have misconfigured or outdated security.**

## Protecting Data in the Cloud

Confidential information stored in cloud services, whether for archival or operating purposes, must usually meet minimum requirements imposed by industry-governing bodies. PCI in the payments space and HIPAA for healthcare data mandate minimum encryption standards for data that is processed or stored.

These standards often require ongoing audits by external parties to ensure continuing compliance. When in doubt about the ways a service provider protects your confidential information, always ask for their security practices.

No matter how your firm stores your data, whether on a cloud storage device or on your computer's hard drive, you need to take steps to ensure that it is secure. Getting sensitive data out of your hands makes it easier on you. Fortunately, there are numerous software programs and systems in place that can help you make sure all the data in your office stays safe and private. For example, with LawPay, you never have to handle sensitive payment details again. Clients can enter their own information through your custom payment page, and we handle the rest. With over a decade of experience in payment technology, we know what it takes to keep data secure. All payments are managed through LawPay's proprietary vault to maximize security and eliminate the risk of storing payment information in your firm.

# Conclusion

The responsibility you have to protect your firm's and your clients' sensitive data is significant, but fortunately, taking steps to protect this data is well within your ability. By prioritizing the security steps covered in this e-book, from your network to your passwords, systems, and data, your law firm will be on a much stronger security footing.

Remember, security optimization is not a one-time event. As technology changes, new threats continue to emerge, but the underlying principles and practices discussed in this e-book will continue to apply. As your office changes over time, keep your asset inventory up to date, and use the steps of this guide as a simple checklist for maintaining the security of your practice.

# The LawPay advantage

Over the past 15 years we have built a reputation as the go-to payment solution for firms of all sizes and established the tool as a pillar of the business technology suite. In addition to easy, secure online payments, LawPay provides your firm with:

- Guaranteed IOLTA compliance for card and eCheck payments
- Advanced fraud and risk protection, including cross-border
- Complete PCI audit and certification program at no extra cost
- Fully integrated eCheck/ACH payments
- Control access levels for individual staff members
- Enhanced reporting tools provide business insights
- Invoice uploader allows for bulk client billing
- Automate payments with scheduled/recurring billing

## Bar-approved CLE program

To benefit your practice and team, the LawPay program includes monthly webinars approved for CLE credit. CLE topics cover a range of subjects including compliance, best practices, communication, fiduciary duties, and ethics. View our full CLE webinar catalogue at lawpay.com/resources/webinars.

AILA
AMERICAN IMMIGRATION LAWYERS ASSOCIATION

**866-492-7515 | lawpay.com/aila**