THE LAW FIRM GUIDE TO

Cybersecurity

Avoiding Damage and Disclosure
Within Your Practice

WASHINGTON STATE
BAR ASSOCIATION

The Law Firm Guide to
CYBERSECURITY
Avoiding Damage and Disclosure in Your Practice

WASHINGTON STATE
BAR ASSOCIATION

The Law Firm Guide to Cybersecurity
Avoiding Damage and Disclosure in Your Practice

Product of the WSBA's Practice Management Assistance Program

www.wsba.org/pma

1325 4th Avenue, Suite 600, Seattle, WA 98101-2539

If you have any questions about this resource, please contact us at pma@wsba.org or schedule a consultation at www.wsba.org/consult.

REPRODUCTION

DISCLAIMER

The Washington State Bar Association (WSBA) provides this guide for informational purposes only; the WSBA does not warrant the information provided with regard to accuracy or any other purpose. No endorsement is intended. The information contained herein does not constitute legal advice or legal opinions.

You are responsible for ensuring your own legal and ethical compliance. Any use of the materials herein is not a defense against discipline, a malpractice claim, or other legal proceeding. This guide does not modify the rules, statutes, and regulations set by the federal government, state legislature, Washington Supreme Court, or the Bylaws and policies of the WSBA, or confer any additional rights.

050520-v1

Contents

Introduction

CYBERSECURITY MAY FEEL LIKE the last item on a long list of considerations for running your law firm and practicing law. What you may not realize is that your firm is vulnerable right now, as you read this, if you have not incorporated basic best practices to guard data and information.

The goal of this guide is to help you understand the issues and trends affecting law firms, and to provide simple, practical resources for you to safeguard yourself and your clients.

In discussing cybersecurity, this guide will cover the common issues and risks for law firms with the use of technology. Generally, the technology tools discussed here are recommended—or even necessary—to effectively practice in today's legal marketplace. However, if you do not know what the best practices are for using these technology tools, you could be putting your practice, and your clients, at risk.

Learning Objectives

This resource will cover these topics:

- Your professional obligations for cybersecurity
- Common misconceptions about technology
- Best practices for securing documents and information

Is This Guide for Me?

WHAT IT INVOLVES:

Cybersecurity is a broad term that generally refers to the protection of systems and information connected to the Internet.

WHAT COULD GO WRONG:

Hackers are increasingly targeting law firms because they can become a one-stop shop for a variety of sensitive documents and information. There is also a growing trend of "ransomware," where a hacker encrypts firm files so that they are inaccessible, and then demands a ransom in exchange for restoring access to the files.[1]

YOU'RE VULNERABLE IF:

- You use the same password for everything.
- You don't know what "phishing" means.
- You transmit confidential documents or Personally Identifiable Information (PII) without safeguards.[2]
- Your clients do the above.

WHAT YOU CAN DO:

- Encrypt files and information
- Use a secure messaging system
- Follow best practices in information management ■

---

[1] For a discussion of cyber attack trends for small businesses, see Patrick Thielen and Dave Charlton, *Cyber Attack Inevitability: The Threat Small & Midsize Businesses Cannot Ignore,* CHUBB (2019) (available at https://www.chubb.com/us-en/_assets/doc/2019_01.31_cyber_whitepaper_chubb_r3.pdf).

[2] "PII" is Personal Identifiable Information, , which is any information about an individual including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. See: Erika McCallister, Tim Grance, & Karen Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" ES1, NIST, available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf.

Your Professional Obligations for Cybersecurity

THE UNDERLYING PRINCIPLES of professional responsibility apply to a modern law office. If you are using mobile devices or cloud services, you have these fundamental responsibilities:

1. **Protect Confidentiality.** You have a general duty to keep all client information confidential.[3] This guide will discuss various ways that digital information can be vulnerable to disclosure, and you need ensure that you are preserving confidentiality in a digital environment.

2. **Competency.** Under your obligation to provide competent representation one thing you are required to do is keep yourself apprised of changes in technology.[4]

3. **Supervise Your Staff.**[5] This is true regardless of your connection to the Internet, but you have a responsibility to adequately supervise your staff. In terms of cybersecurity, this means that you should make sure they are following best practices (see discussion in following sections). It also means that you should be aware of any devices that are being used to access or store client data.

For more information about your ethical responsibilities, contact the WSBA Ethics Line at (800) 945-9722 and refer to WSBA Advisory Opinions 201601 and 2215. ■

---

[3] See RPC 1.6 (or, for Limited License Legal Technicians (LLLTs), LLLT RPC 1.6); RPC 1.15A (or, for Limited License Legal Technicians (LLLTs), LLLT RPC 1.15A).

[4] See RPC 1.1, Comment 8 (or, for LLLTs, LLLT RPC 1.1).

[5] See RPC 5.1, 5.2, 5.3 and 5.10. For LLLTs, see the LLLT RPC 5.1, 5.2, and 5.3.

Get Into the Cloud ... Safely

Cloud-Computing Explained

THE TERM "CLOUD COMPUTING" is a term that encompasses different types of computing resources (such as applications, storage) that are made available by a service provider for convenient, on-demand network access. Although "cloud" implies something magical or ethereal, cloud computing is generally just a form of service that leverages large, centralized data centers for those computing resources. Examples of cloud computing include Amazon AWS, Google Docs, and Microsoft Office 365. Many companies providing services to attorneys offer cloud services.

A common type of cloud service is **Cloud Storage**. Cloud storage is a simple way to "store, access, and share data over the Internet."[6] In other words, it is a method of storing data electronically so that the data is accessible anytime, from anywhere. When you use a cloud-storage service, instead of using your computer's hard drive or a networked server that you have to maintain, you pay a company to store that data on its servers. Examples of cloud storage include OneDrive for Business, Google Drive for Business, and Dropbox.

Some lawyers believe they are not using cloud services. But, if you have an email address that you access through a web browser or an app which ends with a domain address such as outlook.com, gmail.com, you are most likely already using the Cloud for your email data. You are also using the cloud if you use any kind of web application for which the data is not stored on your drive, or a local copy is stored on your hard drive but syncs with a copy stored at a hosted service data center. (This includes most practice management software, project management apps like Trello, and web-based budgeting software like QuickBooks Online).

[6] AMAZON WEB SERVICES, What is Cloud Storage? (https://aws.amazon.com/what-is-cloud-storage/)

Provided you are selecting a vendor with adequate security practices, cloud storage is an excellent way to improve your efficiency and ensure that you are protecting files from inadvertent destruction.

Often, attorneys who do not utilize cloud services (or who think they do not utilize cloud services) are worried about security and confidentiality. That is a reasonable concern, since WSBA members have an explicit duty to maintain confidentiality as well as a duty of technology competency.[7] However, cloud storage could be one of the most secure options for most solo and small firm attorneys, so long as you understand the Service Level Agreement, Terms of Service, and Privacy Policy of your hosted service providers; keep yourself apprised of the trends in the industry; and take adequate efforts to ensure you are following best practices. ■

[7] For more information, review WSBA Advisory Opinions **2215 (2012)** and **201601 (2016)**.

Key Considerations for Secure Data Management

USING A CLOUD SERVICE (as opposed to storing data on your own server or hard drive) may be an ideal security option for solo and small-firm practitioners.[8] In selecting a cloud service, there are a few key considerations. You also should incorporate these principles regardless of whether you use the cloud or rely on your own storage.

You're Still Responsible for Local Security

Even when you use Cloud or hosted services, you are still responsible for the security of your local devices and your portion of the network you use to connect to your Internet Service Provider (ISP), such as Frontier, Comcast, or CenturyLink.

If you work from home or share a physical office with other lawyers in a different firm, then you should have a firewall and use the firewall to separate your networks into separate virtual local area networks (vLAN). A firewall is a device or program that controls the flow of network traffic between two networks or a device and a network that employ differing security postures.[9] For example, a hardware firewall is often installed between the Internet, and a local area network in a home of office. Consider the case where an attorney practices from their home. Their ISP is Comcast, so they have a cable modem. The attorney could install a firewall to the cable modem, and then have a network with the firm devices (desktops and computers) isolated on it; and a separate network for other devices, such as the Smart TVs, and other non-work devices.

---

[8] In rare cases, your practice area may require an exception. Because cloud storage means that data is stored on a third-party's servers, you may want to avoid using a cloud service if you need to be concerned about government surveillance of some kind. This would be an exceptional case and you should consult with a technology expert to devise a protocol that will work for you.

[9] Karen Scarfone, Paul Hoffman, "Guidelines on Firewalls and Firewall Policy," ES-1, NIST, available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf.

Keep Your Systems Updated

You need to ensure that the operating system on your devices is up-to-date with the latest security patches. For example, if you use a Windows Computer you should be running a supported version of Windows (typically Windows 10). If you are using a Mac, you should be running the latest version of macOS. If you access the hosted services from mobile devices such as a smartphone or tablet, they should be running the latest version of the relevant OS.

Some people fail to update the latest security patches because they believe it makes the computer system slower or less efficient. Sometimes, patches do create temporary computing errors. However, those security patches are critical for addressing known vulnerabilities on your devices, so you should always take advantage of available security upgrades.

Use an Anti-Malware Program

Malware is malicious code that is, unbeknownst to the user, inserted into another program with the intent to destroy your data, run malicious programs, or otherwise compromise the confidentiality, integrity, or availability of your data and devices.[10] Windows 10 includes anti-malware software built in (Windows Defender), and third-party anti-malware solutions are available for macOS and Android systems.

Encrypt Wherever You Can

Data you are saving needs to be encrypted. Encryption is a process to secure data from prying eyes.[11] At its most basic level, encryption is a way of making it difficult and time-consuming for unwanted parties to gain access to information. It works by taking information and encoding it so the information is gibberish to anyone who does not have the encryption "key."

---

[10] Murugiah Souppaya, Karen Scarfone, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops,"vii, NIST, available at **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf**.

[11] David G. Ries, Sharon D. Nelson & John W. Simek, Encryption Made Simple for Lawyers (2012).

Your computer's hardware configuration may allow you to easily encrypt your hard drive. For example, Apple users can use FileVault to encrypt everything on their computer.[12] The similar protection on Windows devices is provided by BitLocker.[13] Encrypting your hard drive is a critical first step.

Encryption in Transit

For cloud services such as document storage and email, most if not all such services provide encryption **in transit**. This means that while data is transmitted over the Internet, the information is encrypted and protected from third-party view. If you are using cloud services you need to understand the Service Level Agreement (SLA) and Terms of Service to ensure you know whether or not data is encrypted in transit, and what steps if any you must take to enable such encryption.

Encryption at Rest

Once data is transmitted to the cloud (the service provider's servers) the data may be decrypted to be stored on the vendor's servers. This means that data is viewable to anyone who has access to those servers, including any hackers that gain access (however unlikely that may be). For optimal security, make sure that any cloud service you use offers encryption in transit, but also encryption **at rest**.[14] This means that the information is encrypted as it sits on the cloud vendor's servers. Understand whether that is offered standard, or if you need to opt in to that in the software settings.[15] As of this writing, Google Drive for Business, Dropbox, and Microsoft OneDrive for Business are vendors that offer encryption in transit and at rest.

---

[12] See generally *"Use FileVault to encrypt the startup disk on your Mac"* Apple, available at **https://support.apple.com/en-us/HT204837.**

[13] Chris Hoffman, *How to Enable Full-Disk Encryption on Windows 10*, How-To Geek (Jan. 11, 2017) (**http://bit.ly/2x3P3Vq**)

[14] If you serve a client population that is especially vulnerable in the case of government subpoenas, etc. (such as immigrants) you need to be more concerned about data encryption than most attorneys and you may want to consider a zero-knowledge service. Please contact the Practice Management Assistance program (**www.wsba.org/consult**) to discuss.

[15] See Sharon Nelson & Jim Calloway, *The Cloudy Ethics of Cloud Computing*, THE DIGITAL EDGE (Aug. 29, 2018 Legal Talk Network) (**http://bit.ly/2N8x9ea**).

Encrypting Email

Unfortunately encrypting your email is not straightforward. While some email services allow you to encrypt messages between you and the recipient, it can reduce the convenience of using traditional email services. If you arrange it with your client in advance, you can take simple steps like require a password to view communications. If the password becomes known by a third party, they would have access to your communications.

The simplest approach for secure messaging is to limit your email use to sharing information not highly sensitive. If you are transmitting documents or information that contains things like attorney-client confidential communications, Personally Identifiable Information (PII) (birthdates, social security numbers, addresses, bank account numbers, etc.) or trade secrets and non-public information, you should choose a different method to transmit that information.

Methods of Transmitting Sensitive Information Securely

- For sensitive information, you can either utilize secure email settings (e.g. Gmail allows you to set a password for individual emails you send), or you can use secure messaging services.
- For communicating between you and your client, one of the easiest ways to use secure messaging is to utilize client portals in practice management software. Usually your client would have to enter a unique username and password before they can view correspondence or documents from you.
- For sharing with third parties (outside counsel, experts, etc.) you can use password-protection on files to ensure that only individuals with the password can view the data.

Encourage your clients to adopt best practices for managing the electronic information related to their case. That means making sure they use good, unique passwords for their email or accounts, and setting up their devices so they are not vulnerable if their phone is lost or stolen.

Restrict Remote Access

One of the appealing features of cloud services is that you can access your data from anywhere with an Internet or data connection. Cloud services also make it easy to collaborate with your co-workers and share files externally.

Because cloud services make it easier for you to access data from anywhere, it also becomes easier for a third party to access your data from their own device. This is not a defect of the cloud service. Instead, it is dependent on the access controls you put in place for your accounts and devices.

The ability to access information from anywhere gives you greater flexibility, but it also may cause you to expose client information. This is especially true when you use public wireless connections to access the Internet (such as working in a coffee shop or on an airplane).[16] Public WiFi is still considered "public" and "unsecured" even if you receive a password to connect to the Internet (such as a guest code at your hotel).

When your device accesses public WiFi the data that is being shared over the Internet becomes vulnerable to third-party snooping.[17] **Virtual Private Networks (VPNs)** work by creating an encrypted tunnel so that the information traveling over the Internet is protected from view by other people on that public WiFi network.[18] You should install a VPN on any device that you use to access public WiFi. You should try to select a VPN that does not log any information that passes through it. This means you should likely avoid "free" VPN services which may be ad-based or may collect your user data, instead opting to pay for the VPN software.

---

[16] Steven Petrow, *I Got Hacked Mid-Air While Writing an Apple-FBI Story,* USA Today (Feb. 24, 2016) (**https://www.usatoday.com/story/tech/columnist/2016/02/24/got-hacked-my-mac-while-writing-story/80844720/**)

[17] This includes calls made over WiFi: see Tian Xie, et. al., *The Dark Side of Operational Wi-Fi Calling Service*s, available at: **https://www.egr.msu.edu/~mizhang/papers/2018_CNS_WiFiCalling.pdf**.

[18] Tom Mighell, *Keeping Communications Confidential with a VPN,* LAW PRACTICE DIVISION (September/October 2017) (**http://dashboard.mazsystems.com/webreader/51548?page=32**); Megan Zavieh, *VPN: A Simple Step Toward Cybersecurity,* ATTORNEY AT WORK (Apr. 12, 2018) (**https://www.attorneyatwork.com/vpn-simple-step-toward-cyber-security/**).

The second thing you need to implement is something called **remote wipe** for any mobile device (smart phones, laptops, etc.) that has access to firm data or client information. Remote wipe allows you to delete files and information from a device even if you have lost physical access to it. So for example, if you lose your phone on the bus, you can wipe the data before anyone can access it. Any device you use (or your employees use) should be able to be wiped remotely. Otherwise, those devices should not be permitted to hold, or connect to applications that hold, client information (including email).

Require Two-Factor Authentication

The next step in your security protocols is to make sure you are protecting the login process with two-factor authentication. Two-factor authentication (also sometimes called "multi-factor authentication" or "two-step verification") is utilizing at least two separate mechanisms for confirming your identity before you can gain access to the account.

Usually two-factor authentication means you have to (1) enter your password, and (2) verify your identify by doing something like answering a secret question, or entering a code that is texted to your phone. You can also use an authenticator app on your phone.

Most service providers will allow two-factor authentication, and you should always opt-in to two-factor authentication when that is an option. If employees have access to client data or information on their mobile devices, they should have to utilize two-factor authentication, preferably using phones securely locked with either their fingerprint or with complex passwords.

Cloud Service Checklist

For a checklist to select a cloud service provider, visit **www.wsba.org/guides**. Because technology changes constantly, you should keep yourself apprised of changing Service Level Agreements, Terms of Service, Privacy Policies, and industry standards, and ensure that the service you use is meeting those standards.

Use Best Practices for Passwords

The recommended practices for passwords have changed. This is because (1) technology advances all the time and (2) people follow similar patterns, such as using pop culture references, that make passwords vulnerable.[19] In June 2017, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) provided guidance for password creation.[20] Here are key takeaways:

1. **Long Passwords Required.** Password length is the primary factor of password strength. If your password is too short, it is vulnerable to brute force attacks (when an attacker tries many passwords or phrases hoping to guess correctly). Most people create passwords of 8–12 characters in length. Importantly, an advanced intruder can crack an eight-character password in about six hours.[21] To make your passwords less vulnerable, you should use passwords, or pass phrases, that are 25 characters long (or as long as you can depending on the password restrictions set by the vendor).
2. **"Password" is a Terrible Password.** At this point, most people know that it is a terrible idea to use the word "password" within your actual password. However, even if you do not do that, you may still include common patterns or words easily guessed.[22] For best results, do not use common dictionary words in your password and never use the name of your firm or the hosted service itself. It is better to use words or phrases uniquely relevant to you, and are not readily available from public records (e.g. your children's names, birthdates, your address, etc.).

---

[19] See https://www.wired.com/2016/05/password-tips-experts/ quoting a CEO of a password management company. You should avoid pop culture references, regardless of the length of your password.

[20] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Digital Identity Guidelines* (June 2017) (https://pages.nist.gov/800-63-3/sp800-63b.html#appA). See also Samantha Raphelson, *Forget Tough Passwords: New Guidelines Make It Simple,* NATIONAL PUBLIC RADIO (Aug. 14, 2017) (https://n.pr/2CFmIKh)

[21] See the calculator widget by Better Buys at https://www.betterbuys.com/estimating-password-cracking-times/.

[22] For examples, check out Cara McGoogan, *The world's most common passwords revealed: Are you using them?,* THE TELEGRAPH (Jan. 16, 2017) (https://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/) and WIKIPEDIA, *List of the most commons passwords* (last updated Sept. 7, 2018) (https://en.wikipedia.org/wiki/List_of_the_most_common_passwords).

3. **Don't Repeat Yourself.** Every password you use should be unique. That means you should not use the same password for multiple accounts or services. The reason for this is that it makes it easy for someone to gain access across your various accounts if they just have one log-in obtained by a breach or other method. Every password is the opportunity to add a locked door. Do not duplicate the key.
4. **Don't Force Changes in Password.** Recent studies show that constantly changing passwords may cause more problems than it prevents. Some systems force the use of a new password every 60 days. If you are following the first three recommendations, you may wish to stop forcing or frequently changing your password or the passwords of your employees.[23]

Passwords should be used not only for applications and for software, but also on the devices you use to access those applications and software. This includes your computer, laptop or tablet, and mobile devices. Otherwise, third parties could access your data and files stored locally without even needing your web passwords.[24]

[23] See generally, "Security baseline (FINAL) for Windows 10 v1903 and Windows Server v1903— Dropping the password expiration policies", available at **https://blogs.technet.microsoft.com/secguide/2019/05/23/security-baseline-final-for-windows-10-v1903-and-windows-server-v1903/**.

[24] Most cloud services will store data "locally" on your devices, meaning that data is downloaded from the Internet onto your device so that you can access it even when you are not connected to the Internet. When you are connected to the Internet, your device will transmit data back and forth with the cloud service.

▶ *Password Managers*

If you follow the above advice, it will be difficult (if not impossible) to keep track of these passwords and actually remember them all. Fortunately, you can use an encrypted password manager that will allow you to securely keep track of your passcodes using one primary password. Examples include Keychain, LastPass, and 1Password. For more, check out:

- Chris Hoffman, *Why You Should Use a Password Manager, and How to Get Started,* HOW-TO GEEK (Dec. 12, 2016) (**https://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/**)
- Eric Limer, *You Should Be Using a Password Manager*, POPULAR MECHANICS (May 24, 2017) (**https://www.popularmechanics.com/technology/security/a26629/use-password-manager/**)
- Cara McGoogan, *Is it safe to use a password manager?*, THE TELEGRAPH (Apr. 4, 2017) (**https://www.telegraph.co.uk/technology/0/safe-use-password-manager/**)

Some password managers integrate with MFA devices or keys, which provide additional protection, including using biometrics. For example, Google and Yubico make specialized USB-like devices which integrate with password managers.[25] ■

[25] For examples, check out Google Titan, available at: **https://cloud.google.com/titan-security-key/** or Yubico key available at **https://yubico.com**.

Special Case: IoT Devices

AN IoT (Internet Of Things) DEVICE is any appliance, gadget, accessory, or other physical item that connects to the Internet.[26] Examples of IoT devices include:

- **IoT wearables** such as smart watches or step counters.
- Virtual assistant services and hardware such as the Amazon Echo and Google Home.
- Home monitoring equipment such as a nanny cam or pet camera.

An IoT device for your practice can help you run a more efficient law office. For example, you can use a Virtual Assistance service to help you track your time, complete tasks, and more. But if you use an IoT device (whether at home or at work) you may be opening yourself up to cybercrimes:

- An IoT wearable can allow data access if it is lost or stolen.[27]
- Innocuous devices like smart lightbulbs and coffeemakers can expose your Wi-Fi password.[28]
- Some devices are monitored by the service provider and could create logged data subject to subpoena or create issues related to confidentiality and attorney-client privilege.

---

[26] Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, Forbes (Mar. 13, 2014) (https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#100450dc1d09)

[27] Kirk McElhearn, *Apple Watch Security and Privacy Tips*, INTEGO (Jan. 10, 2018) (https://www.intego.com/mac-security-blog/apple-watch-security-and-privacy-tips/)

[28] Dan Goodin, *Crypto weakness in smart LED lightbulbs exposes Wi-Fi passwords*, ARS TECHNICA (July 7, 2014) (https://arstechnica.com/information-technology/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/); Steve Ranger, *The spy on the corner of your desk: Why the smart office is your next security nightmare*, ZDNet (Mar. 1, 2018) (https://www.zdnet.com/article/the-spy-on-the-corner-of-your-desk-why-the-smart-office-is-your-next-security-nightmare/)

If you are using an IoT device within the scope of your practice (whether at the office or at home when you work remotely), you need to make sure your devices are set up securely and that you are using them consistent with the best practices described here. That means that you use unique and strong passwords (see **"Use Best Practices for Passwords" on page 12**) for each device and prioritize services that use robust encryption. Again, it is necessary to fully understand the Service Level Agreement, Terms and Service, and Privacy Policies for all such devices.

In addition, because IoT devices are especially vulnerable to malicious attacks, also take these precautions:

1. **Just Say No:** if an IoT device you are considering does not allow you to update its software or firmware, or change the password, avoid purchasing it.[29]
2. **Separate Your Network:** Your Internet network can be compartmentalized so guests using your WiFi do not get access to the main network.[30] Similarly, create a separate network for your IoT devices.[31]
3. **Limit BYOD at Work:** Besides your own devices, if you have employees you also need to consider what devices they are bringing to work, and what devices they are using to review or access firm data. Your employment agreement should set out guidelines for staff.

■

[29] Rob Marvin, *The 5 Worst Hacks and Breaches of 2016 and What They Mean for 2017,* PC MAG (Jan. 7, 2017) (**https://www.pcmag.com/article/350793/the-5-worst-hacks-and-breaches-of-2016-and-what-they-mean-fo**).

[30] Bradley Mitchell, *Setting Up and Using a Guest Wi-Fi Network,* LIFEWIRE (Mar. 19, 2019) (**https://www.lifewire.com/guest-network-for-home-tutorial-818204**).

[31] Mark Dacanay, *Common Sense Security Tips for IoT in the Office,* GLOBALSIGN BLOG (Apr. 24, 2018) (**https://www.globalsign.com/en/blog/cybersecurity-tips-for-office-iot/**)

Special Case: Email Phishing

PHISHING IS A CYBERCRIME in which a hacker poses as a legitimate institution or person to "lure" someone into providing sensitive information such as passwords, bank account information, etc.[32] Hackers can also pose as a legitimate sender to lure a recipient to open a file or web link that causes malware to be downloaded to the computer (also known as a "malicious link").[33]

Lawyers are vulnerable to these schemes because most people are not using basic best practices for email security, and hackers know that law firms are a prime target for hacking. For example, a hacker may gain access to a client's account, and then masquerade as your client mislead you and your staff. into misdirecting settlement funds to a different bank account.

Don't Take the Bait

Before you click a link or download a file you receive via email, make sure it is what it purports to be. Here is an example phishing email:

I tried sending you this doc earlier but noticed the failure delivery so had to re-send it securely.

Kindly view below:

116Kb

PDF <https://smarturl.it/8vaw26> | Preview <https://smarturl.it/8vaw26>

Download <https://smarturl.it/8vaw26>

[32] PHISHING.ORG, *What is Phishing?* (Accessed Sept. 12, 2018) (**http://www.phishing.org/what-is-phishing**).

[33] Michigan State University, College of Engineering, *How to Recognize a Malware Email* (Accessed Sept. 12, 2018) (**https://www.egr.msu.edu/decs/security/how-recognize-malware-email**).

The message was followed by a signature block from a WSBA member that looked valid—it had his WSBA number, his address, his phone, etc. However, the recipient was not expecting any documents from this person, and the format and phrasing was somewhat unusual. If you receive an email like this, these are all warning signs that should prompt you to call the sender to make sure they actually transmitted a message to you. Here, the member's email account had been compromised and a third party was using it to send phishing emails.

To protect yourself from similar issues:

1. **Make Sure They Are Who They Say They Are.** Some phishing schemes rely on tricking you into believing the sender is coming from a trusted domain, when in fact there are clues to suggest otherwise. Check the sender's email address (not just the display name) and look for inconsistencies in the domain name. For example, instead of "@becu.org" the sender's domain might be "@becu-company.com."

2. **Give Unexpected Items More Scrutiny.** Before you click on a link or open an attachment you received, make sure you consider whether it was something you were expecting. If not, call the sender on the phone (do not verify by email!) to confirm that the document or link is authentic. Unsolicited invitations to view or access a document may be phishing schemes.

3. **Inspect Links.** A hyperlink has two elements: the text displayed (what you see on the screen), and the actual URL (web) address you will be directed to when you click the link. For example, if you are viewing these materials electronically, hover your mouse over **this link** until you see the text of the URL address. It is also possible to create a link that displays one address, but directs you somewhere else (e.g. **https://www.wsba.org/pma)**. Never click a link you have not inspected first.

4. **Disable Macros and Protect Files.** This is an easy step you can take right now. For all of your Microsoft Office products, make sure that your settings are set so that (1) macros are disabled and (2) documents from the Internet are opened in "protective view."[34]

5. **Don't Give Identifiers Away.** Some phishing schemes may ask you to respond to an email with your sensitive information like your social security number, or answers to your secret questions. Do not provide sensitive information unless you have verified the authenticity of the service provider and the data is remitted securely.[35] ■

[34] Specific steps for these items will vary depending on your software. You can find information on how to do this within the Help resources in your program, or you can contact us for assistance at pma@wsba.org.

[35] For more information about verifying the security of the website (e.g. checking the SSL certificate), see Joyce Tammany, *How Can I Tell If a Website Is Safe? Look For These 5 Signs,* SITELOCK (Aug. 24, 2018) (https://www.sitelock.com/blog/is-this-website-safe/).

TL;DR[36]

WHETHER OR NOT you realize it, you probably are already using cloud services. With any technology or electronic information, the RPCs require you to: (1) protect the confidentiality of client information, (2) supervise your staff's use and access to that information and (3) stay apprised of technology changes that impact your ability to competently provide legal services. ■

[36] A shorthand notation summarizing the content of the materials.

Glossary

Term/Acronym	Definition
BYOD	"Bring Your Own Device" refers to employees using personal devices (computers, phones, etc.) to connect to workplace Internet or access firm data.
Cloud Computing	Broad term that encompasses different types of computing resources (such as applications, storage) that are made available by a service provider for convenient, on-demand network access
Cloud Storage	The method of storing, accessing, and sharing data over the Internet.
Encryption	A process of securing data that makes it more difficult for third parties to gain access to the data. Data can be encrypted as it is sent or received over the Internet (encryption "in transit") or while it is stored (encryption "at rest").
Internet of Things (IoT)	Any appliance, gadget, accessory, or other physical item that connects to the Internet. Includes IoT Wearables, such as smart watches.
ISP	Internet Service Provider; your ISP is the company that you pay for Internet access.

Macro	A sequence of computing instructions recorded as a single step. The concept is that you can automate routine or tedious steps for greater efficiency, but malicious actors can also record macros that will harm your computer or cause a data breach.
Malicious Link	A hyperlink or attached file that, when clicked or opened, will cause malware to be downloaded to the user's computer.
Malware	Malicious code that is, unbeknownst to the user, inserted into another program with the intent to destroy your data, run malicious programs, or otherwise compromise the confidentiality, integrity, or availability of your data and devices
Password Manager	A software program that securely stores password and account information.
Remote Wipe	A method of deleting data from a device that you do not have physical access to.
Two-Factor Authentication	Requiring two or more methods of verification before access is permitted. Also called "multi-factor authentication" (MFA) or "two-step verification."
URL	Uniform Resource Locator; better known as a "web address" or "web link."
VPN	Virtual Private Networks (VPNs) create an encrypted tunnel so that the information you send or receive over the Internet is protected from view by other people connected to the same WiFi network.

Additional Resources

Frequently Asked Questions

- *I use Apple devices. Do I need anti-malware?*

Yes. Although most malware targets the Windows operating system, bad actors are developing malicious code that targets the mac operating system as well.

- *Is it okay to use a cloud-based service?*

With some exceptions, cloud computing may be a very secure option for you if you follow best practices for cybersecurity.

WSBA Member Resources

For more information and assistance from the WSBA, consider these resources:

- **Free Lending Library:** Borrow from a selection of 400 books. You can register immediately online and start placing holds. Titles will be shipped to you automatically. Visit **www.wsba.org/library** to get started.
- **Free Consultations:** You can speak with an advisor in the Practice Management Assistance program for personalized advice regarding your law firm business management. Visit **www.wsba.org/consult** to get started.
- **Free Ethics Help:** You can speak to WSBA staff regarding questions of ethical obligations and your professional responsibility. The phone number is (800) 945-9722.
- **Discounts on Software and Services:** Through the Practice Management Discount Network, WSBA members receive discounts on a menu of software and services to help you improve your practice and client service delivery. Visit **www.wsba.org/discounts** to learn more.

For more resources, visit **www.wsba.org/MemberSupport**. ■

WASHINGTON STATE
BAR ASSOCIATION