Securing Your Digital Practice: Essential Password Strategies for Attorneys

Lawyers must take the appropriate foundational steps to defend against cyberattacks. This article discusses strategies for securing lawyer and law firm online accounts through robust password practices, password managers, multifactor authentication, and policies.

BY BRENT J. HOEFT

The buzz of generative artificial intelligence (GAI) is everywhere, and the legal industry is no exception. However, all the features that GAI brings as a tool for the practice of law also benefit bad actors who are trying to deceive their targets into providing access. GAI allows bad actors to create more convincing phishing emails while expending less time, effort, and expense. Anyone is susceptible to falling for one of these scams. Not even security professionals can be right all the time.[1] Therein lies the problem – the bad guys only need to be right once; the rest of us have to be right 100% of the time.

Law firms are prime targets for cybercriminals because of the sensitive client information law firms possess. The first quarter of 2024 saw nearly as many law firm data breaches as the entirety of 2023.[2] For attorneys, protecting digital assets is not just best practice – it's an ethical obligation.[3] Therefore, it is necessary to make sure that lawyers are taking the appropriate foundational steps to have the best chance to defend against these attacks. This article discusses strategies for securing lawyer and law firm online accounts through robust password practices, password managers, multifactor authentication, and policies.

Password Best Practices – Going Beyond 123456: Creating Strong Passwords

The foundation of account security begins with strong passwords. Unfortunately, humans are notoriously bad at strong passwords in practice. The top three commonly used passwords in 2024 were 123456, 123456789, and 12345678.[4] It is no surprise that these are not strong passwords. There are certain characteristics that all strong passwords should have.[5] A strong password should:

- Contain at least 15 characters.
- Include a mix of uppercase and lowercase letters, numbers, and symbols.
- NEVER be reused. Each account must have its own unique password.[6]

Consider using passphrases rather than passwords – longer combinations of words that are easier to remember but difficult to crack. For example, a phrase like "1BeachfrontLegalWork@SunsetFire2025!"is both memorable and secure. With the number of online accounts that people are managing, by some estimates an average of 168 total online

Brent J. Hoeft, Cleveland State Univ. College of Law 2006, is the State Bar of Wisconsin's practice management advisor and manager of the Practice411™ practice management program. If you have questions about technology, practice management, or the business aspects of your practice, call (800) 957-4670 or email practicehelp@wisbar.org. Access the digital article at www.wisbar.org/wl.

accounts and 87 business related,[7] it is impossible to remember them all. Enter, the password manager.

Password Managers: Your Digital Vault

As mentioned, the average person manages an estimated 168 passwords as of 2024 — an increase of nearly 70% over the last three years.[8]

Password managers can do all the following:

• Generate complex, randomized, unique passwords — and now passphrases — for each account.

• Securely store all your credentials in an encrypted vault.

• Auto-fill login information, saving time, reducing friction, and increasing security because the password manager will only provide an auto-fill option on websites that users already have associated with their accounts.

• Identify weak, reused, or known-compromised passwords.

• Help users share credentials securely when doing so is necessary.

Password managers function as complete systems rather than single applications. They typically include apps and browser extensions for all the user's devices that help create, store, and evaluate the security of passwords. This information is encrypted and synchronized across devices through secure servers.

When a user visits a website, the password manager can automatically fill in the user's stored credentials. If the user creates a new account or changes a password, the password manager offers to save or update this information. Finally, password managers can alert users to potentially compromised passwords after data breaches and facilitate quick password changes.

Selecting password managers. When selecting a password manager, ensure that it:

• Works across all devices you use,

• Offers secure syncing between devices,

• Provides strong encryption,

• Includes breach monitoring,

• Supports multifactor authentication for the password manager itself, and

• Has a user-friendly interface.

The following are a few popular and recommended password managers[9]:

• 1Password, https://1password.com

• Bitwarden, https://bitwarden.com

• Dashlane, https://www.dashlane.com

Implementing Password Policies

Law firms should establish clear password policies that all employees must follow. These policies should outline:

• Minimum password length and complexity requirements,

• Password rotation schedules,

• Restrictions on password sharing, and

• Reasons for the policy (the "why") and consequences for policy violations.

Regularly updating passwords reduces the risk of compromise. The same password used for an extended period is more likely to have been exposed in a data breach. Establish a schedule for password changes that aligns with the firm's security policy.

Multifactor Authentication: The Essential Second Line of Defense

Multifactor authentication (MFA) requires at least two verification factors (also known as two-factor authentication or 2FA) to access an account, combining:

• Something you know (password or PIN);

• Something you have (security token, smartphone app, or smart card); and

• Something you are (biometric verification such as fingerprints or facial recognition).

For law firms handling sensitive client information, MFA is not optional — it's an essential security step. Even if a password is compromised, attackers still need the second factor to gain access.

MFA can be implemented through various methods, each offering different levels of security and convenience. Here are three common MFA approaches in order of least secure to most secure:

1) Text, Email, Phone Call Authentication (good security). This method sends verification codes via text message, email, or phone call that users must enter to complete the login process.

2) Mobile Application Authentication (better security). This method uses smartphone applications to verify identity, either through generated codes or push notifications. Examples include Google Authenticator, Microsoft Authenticator, and Duo Mobile.

3) Hardware Security Tokens (best security). Physical devices that generate one-time passwords or provide cryptographic authentication. Examples include the following:

• YubiKey: a physical USB device that generates secure authentication data, highly resistant to phishing attacks.

• RSA SecurID: a key fob that displays a new numeric code every 60 seconds for user authentication.

• U2F USB devices: Universal 2nd Factor authentication tokens that provide strong hardware-based security.

• Bluetooth tokens: wireless devices that can authenticate users when in proximity to the computer or mobile device.

Any of these MFA methods significantly enhances security by requiring additional verification beyond a username and password, making it much more challenging for unauthorized users to gain access to accounts and sensitive information.

Start implementing MFA into your practice by enabling MFA on your most critical accounts first: email accounts (as these are often the gateway to password resets for other accounts), cloud storage services containing client documents, practice management software, financial accounts, and court filing systems.

While some attorneys may find MFA slightly inconvenient, this "annoyance" is actually a benefit — something that inconveniences an attorney also creates a significant barrier for attackers. Going through the extra steps for accessing accounts is a great way to keep security front of mind as attorneys go through their daily routines.

Comprehensive Security Strategy

The first steps to an effective online account security strategy combines all three elements discussed:

- Strong, unique passwords for each account;
- A password manager to generate, store, and monitor those strong passwords; and
- Multifactor authentication wherever available.

This layered approach significantly reduces vulnerability to common attacks.

As with many things security related, account security access is not a "set it and forget it" process. Once set up correctly, account security needs to be frequently revisited to ensure that security is maintained. Law firms can do regular account and password security audits to identify:

- Weak or reused passwords (password managers have these checks built in),
- Accounts lacking MFA,
- Team members not following security protocols who could benefit from additional training, and
- New security services or techniques that should be incorporated into a law firm's security framework.

Training: Securing the Weakest Link

Continuously train all firm personnel on security best practices and the firm's password policy. In an instant, with the click of a finger, the strongest hardware and software security protections can be undermined by human error. Ensure everyone understands:

- How to create strong passwords,
- The importance of not sharing passwords,
- How to recognize phishing attempts,
- Proper use of the firm's password manager,
- MFA procedures, and
- Why all of this is important. To have buy-in from employees or coworkers, you must explain the "why."

Conclusion

The legal profession is particularly attractive to attackers because attorneys and law firms hold valuable personal and financial information for themselves and their clients. Attackers also know that even if confidential information is not inherently valuable to the attacker, all confidential information held by law firms is valuable to the firm and individual attorneys because of attorneys' professional duty to take reasonable steps to prevent unauthorized access by third parties to client information.[10] This awareness by bad actors is a major reason why there has been a proliferation of ransomware attacks directed at the legal industry.

For attorneys, implementing robust security practices is both practical and ethical. Combining strong passwords, password managers, multifactor authentication, policies, and training offers a strong defense against unauthorized access to sensitive client information. No matter the firm size, having account password and access policies is necessary. Training on these policies and explaining why they are necessary is an important step for firm-wide buy-in. Because the legal profession is built on trust and confidentiality, security is not merely a technical consideration – it is a fundamental professional obligation. **WL**

Learn More!

ELEVATE your law practice with actionable guidance from the *Practice Pulse* podcast, produced by the State Bar of Wisconsin and hosted by Practice Management Advisor Brent Hoeft. Listen to expert insights and practical strategies from leading voices across the legal industry, tailored to help you run a more efficient and successful law firm.

Visit: wisbar.org/NewsPublications/Podcasts/Pages/Practice-Pulse-Podcast.aspx **WL**

ENDNOTES

[1]See a story about the successful phishing attack of Troy Hunt, security technology professional and creator of the "Have I Been Pwned" data breach aggregator: *A Sneaky Phish Just Grabbed My Mailchimp Mailing List*, March 25, 2025, https://www.troyhunt.com/a-sneaky-phish-just-grabbed-my-mailchimp-mailing-list/.

[2]Staci Zaretsky, *Biglaw Firms Fall Prey to Cyberattacks, With Data Breaches On the Rise*, Above the Law (May 23, 2024), https://abovethelaw.com/2024/05/biglaw-firms-fall-prey-to-cyberattacks-with-data-breaches-on-the-rise/.

[3]*See* SCR 20:1.1 Competence cmt. 8; SCR 20:1.6 Confidentiality.

[4]*See Top 200 Most Common Passwords*, 2024 Nordpass Research Insights 6th Ed., https://nordpass.com/most-common-passwords-list/.

[5]NIST SP800-63B (Aug. 28, 2024), https://pages.nist.gov/800-63-4/sp800-63b.html.

[6]Unless single sign-on (SSO) has been implemented into a law firm, which is different than reusing the same password across multiple accounts.

[7]Kamile Viezelyte, *Juggling Security: How Many Passwords Does the Average Person Have in 2024?* (April 24, 2024), https://nordpass.com/blog/how-many-passwords-does-average-person-have/.

[8]*Id.*

[9]Scott Gilbertson, *The Best Password Managers to Secure Your Digital Life*, WIRED (March 26, 2025), https://www.wired.com/story/best-password-managers/; *see also* Max Eddy, *The Best Password Managers*, N.Y. Times Wirecutter (updated Feb. 28, 2025), https://www.nytimes.com/wirecutter/reviews/best-password-managers/.

[10]SCR 20:1.6 Confidentiality; *see also* Wis. Formal Ethics Op. EF-21-02: Working remotely (Jan. 29, 2021); Wis. Formal Ethics Op. EF-15-01: Ethical Obligations of Attorneys Using Cloud Computing (amended Sept. 8, 2017). **WL**