SUSMAN GODFREY L.L.P.
HIGH STAKES. HIGH PERFORMANCE.

Essential Digital Privacy Practices For Legal Professionals

In today's world of heightened cyber threats and data breaches, legal professionals must take digital privacy and security seriously. With sensitive client information constantly at risk, now more than ever is the time to implement strong digital habits. Here are actionable steps legal professionals can take to protect their privacy and secure their data.

General Security Practices

1. Use a Password Manager

Strong, unique passwords are your first line of defense against unauthorized access. A password manager, like Dashlane or 1Password, is a cornerstone of digital security. These tools help create, store, and manage complex passwords across all your accounts. Also, avoid repetition. Never reuse passwords across multiple platforms. Each password should be distinct—no shared roots like "client2023!" followed by "client2024!" Use a mix of uppercase and lowercase letters, numbers, and special characters. You should aim for a security score of 90 or above to ensure optimal safety. (Most password managers should have built-in password strength assessors).

2. Enable Two-Factor Authentication (2FA)

Even strong passwords can be compromised—but consistent use of 2FA adds an extra layer of security. Wherever possible, activate 2FA—especially on banking, credit card, and investment accounts. Try to avoid SMS-based codes; they're vulnerable to interception. Instead, use authenticators like Microsoft Authenticator or Dashlane's built-in 2FA. With authenticators, the hardware seed is located on your personal device which is far harder to hack or intercept as compared to SMS text-based codes which are far more vulnerable.

3. Strengthen Your Device Passcode

Your phone or tablet often holds the keys to your digital life—make it harder for hackers to break in. If you're still using a six-digit numeric code, it's time to upgrade. Switch to an 8+ character alphanumeric passcode for significantly stronger protection. Here's a link to Apple's instructions on how to do so.

4. Use a VPN When Away from Secure WiFi

Public WiFi is convenient—but it's a favorite hunting ground for cybercriminals. Whenever you're outside your home or office. particularly while traveling, use a VPN like NordVPN. This is especially critical when connecting to public WiFi in airports and hotels. Be aware that some networks, such as airline WiFi (e.g., United), may restrict VPN usage.

5. Switch Your Search Engine to DuckDuckGo

Most search engines track you—DuckDuckGo doesn't. Replace Google with DuckDuckGo as your default search engine. It doesn't track your searches, providing a more private browsing experience. DuckDuckGo even has a convenient guide to walk you step-by-step through the process of changing your default engine on any browser.

6. Remove Your Data from the Web

You'd be surprised how much of your personal data is floating around online. Use services like DeleteMe to remove your personal contact details from people-search websites like ContactOut, Spokeo, or Whitepages.

7. Secure Your Home WiFi

Your home network should be a fortress, not a revolving door. Your home network can be a vulnerability if not properly configured. To start -- Hide your network name (SSID). Use WPA3 encryption and a passphrase with at least 12 characters. And while you're at it, set up a separate guest network—make it public and isolated from your main devices, and make that the one you offer to visitors and guests so that they never have to bug you for the password.

Privacy Features Every Lawyer Should Enable

8. Protect Your Private Browsing Tabs

Incognito mode is great for peace of mind. But if you want to keep your private Safari tabs truly private, enabling these settings will add a heightened layer of security to your most sensitive browsing.

To protect your tabs, go to Settings > Safari and toggle "Require Face ID to Unlock Private Browsing." Now, after 15 minutes of inactivity, Safari will require Face ID to reopen private tabs.

9. Lock Sensitive Apps with Face ID

Just because someone can hold your phone doesn't mean they should access everything on it. Keep prying eyes out of apps like email, document editors, banking or investment apps, or photo repositories. To enable this feature, long-press an app from the home screen and tap enable Require Face ID. This is perfect if you have kids, family members, or others who often use your phone.

10. Use Guided Access to Lock into One App

Want to lock down your phone even further? The Guided Access feature ensures that whoever you're handing your phone to will only be able to stay in the app you intend. To enable it, navigate to Settings > Accessibility > Guided Access. Once activated, you just triple-click on the app you wish to let another person use and that user will be restricted to that app. This one is a lifesaver for nosy kids – keep your sensitive secrets safe and your peace of mind intact.

11. Enable Stolen Device Protection (iOS 17.3+)

A clever thief can do a lot with your phone—even if they don't know your Apple ID. And though it may sound far-fetched, there have been numerous reports of savvy thieves spying on unwitting marks for long enough to snoop their passcode before swiping the phone. Armed with that critical info, the chances that you are able to recover your device and all the sensitive information it contains are next to none. This powerful feature prevents thieves from wiping or accessing your device even if they know your passcode.

To enable it, go to Settings > Face ID & Passcode > Stolen Device Protection. Once activated, certain sensitive actions—like changing passwords or turning off Find My iPhone—will require Face ID or Touch ID authentication, even if the thief has your passcode. This is a must-have for anyone who absolutely, positively, cannot let their phone fall into the wrong hands.

Final Thoughts

For legal professionals, client confidentiality isn't just a best practice—it's a requirement. It's high time we start treating our own information and data with as much care and consideration. Implementing these privacy and security strategies will not only protect your personal data but also uphold the trust and safety of your clients. In a world where cyber threats continue to evolve, staying one step ahead is not just smart—it's essential.

J. Hoke ("Trey") Peacock III
Susman Godfrey, L.L.P.
1000 Louisiana, Suite 5100
Houston, TX 77002
713-653-7808 (direct dial)

Bio vCard Connect on LinkedIn

About the Author

Trey Peacock, a partner at Susman Godfrey, has been winning cases based on science and data for over 25 years. He has also chaired the firm's IT committee for over two decades. Learn more about Trey **here**.

We all receive too many emails. If you do not wish to be included on future tech notes, please let me know by reply email or click the "Unsubscribe" link below and I will make sure you are removed from any future emails.

Houston | Seattle | Los Angeles | New York

www.SusmanGodfrey.com