

Passwords & Security: An Ethical and Technical Guide for Lawyers

By TREY PEACOCK

In today's world, hardly a month passes without a major technology or web company regretfully announcing a breach of its users' personal data. As remote work becomes more common, issues of security and password protection take on greater importance as work moves outside the safer confines of office network environments.

Security and password protection should be important to any user, but additional ethical obligations require lawyers to protect client information and communications. The Texas Supreme Court recently adopted a change to Comment 8 of Rule 1.01 of the Texas Rules of Disciplinary Conduct which states, "Because of the vital role of lawyers in the legal process, each lawyer should strive to become and remain proficient and competent in the practice of law, **including the benefits and risks associated with relevant technology.**"¹

Implementing strong password protection is one of the most important steps a lawyer can take toward fulfilling the obligation to protect client data. A system of strong, unique, and practical passwords guards your electronic information and communications and serves as one of the most potent lines of defense against inevitable data hacking. This article offers several rules and tips, which are easy to implement and will help safeguard your data, communications, and devices.

How Your Passwords Get Hijacked and Distributed

Many believe the maximum damage that

results from a hack of your Facebook username and password is an embarrassing post or two, and the annoyance of resetting the account. However, the true danger of a hack like the one that occurred at Facebook,² materializes when the tenacious hacker capitalizes on the reality of human user error. All too often, the password to your Facebook account isn't just for Facebook. It's also your Amazon password, and your Wells Fargo password, and it's just one letter or digit off from your work computer network login.

Suddenly, what began as a simple breach of your Facebook account has developed into a full-fledged disaster, allowing a clever hacker to access your address and credit card data stored in your Amazon account, your banking information, and potentially, your entire library of sensitive, confidential legal files. Once the hacker has your information, he can use it in his own phishing or fraud scheme, or sell it on the dark web to other exploiters. The domino effect in cyber form.

Rule #1: Use Lengthy, Complex, Unique, Truly Random Passwords for Each Site

Creating **unique** passwords for each of your online accounts is essential to maintaining the integrity of your data. That way, if one domino goes, the others stand fast. Several criteria factor into the creation of a strong, unique password.

First and foremost, never repeat any password, in part or whole, across more than one account. This includes tacking on characters, numbers, or capital letters. Hackers know that trick too, so just start from scratch. Second, not every account hack arises from a big tech company data breach. Sometimes, hackers employ a "brute force" attack on a user's account. This entails trying dozens of possible password combinations every second until the correct one is reached. The only safeguard against this measure is a password long and complex enough to render a brute force attack impractical. For example, the simple

password "lawyer" would take a modern computer only milliseconds to guess. In contrast, the moderately more complicated password "Law&ryer2" would hold up for weeks or months. The longer and more complex a password is, the harder it is to crack. Thus, a secure password ought to include *at least* 10 to 12 characters, both lowercase and capital letters, and preferably a few numbers and symbols. These additions can increase the amount of time it takes to crack your password exponentially – from a few milliseconds to a few decades.

Rule #2: Use a Password Manager

The point at which I urge the creation of long and seemingly impossible-to-remember passwords for every account, is the point at which many abandon the cause. How can anyone create and remember a complicated, unpronounceable, 12-character password for *every single one* of the dozens of accounts you operate? The answer to this question is also the most useful tool in combating online security breaches: high-performance password manager software such as Dashlane, 1Password, or Keeper.

These password management applications allow users to easily create, store, and retrieve lengthy, randomly-generated passwords for each of their online accounts. Utilizing a single program to store all of your passwords may feel irrational; if all my passwords are in one convenient place, doesn't that make it easier for hackers to get at my stuff? No. These companies combine heightened encryption technologies with your unique Master Password (stored only on your computing device) to protect your passwords.

With the help of a password manager, the savvy internet user need only remember THREE unique passwords: (1) a work or office network password; (2) a single mobile device password (more on that later); and (3) the master password for the password manager. With this set up, a hacker cannot use data gleaned from one account breach to access data in another account.


Rule #3: Create Three Easy to Remember, Lengthy, Complex Passwords

Those three passwords you are going to have to remember still need to be unique, lengthy and complex. To create them, think of an easily-remembered song title, lyric, street name, quotation, or other tidbit of information, and use it as a starting point. For example, say you are a Jimmy Buffet fan. Then, you might start with the lyric “wasting away in Margaritaville.” Compress that, add a few characters, and you’ve got “JBwaiM1946.” Easy enough, right? Compare this complex password, which would take years to brute force, with the simple alternative: “buffet,” which would fold under an attack in only seconds. Utilize this approach for the three main passwords in your daily life and your data will be far more secure.

Rule #4: Change the Passcode on Your Phone and Tablet

Finally, you should implement these same password criteria on your mobile devices. Mobile phones and tablets carry a much greater risk of breach via physical theft than a network does. Yet, as all tech-savvy professionals know, the files contained within these devices are no less confidential or sensitive than the information on your network server. Users should take full advantage of newer devices with fingerprint or facial unlock technology, as they are far harder to beat than a standard passcode. However, users are still required to enter a passcode every 10–14 days, or whenever the device reboots. Thus, you should upgrade the passcodes on your mobile devices to an eight-digit or 10- to 12-character alphanumeric password. You can easily do this by avoiding the default six-digit passcode default and selecting “password options” when changing your password on your device.

You may choose to use all, some, or none of the precautions discussed in this article. Regardless of your current level of security-consciousness, there is a myriad of resources and programs available to help users secure and protect electronic information. Savvy

lawyers understand that ignoring cybersecurity precautions can have far-reaching and long-term consequences. 

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.

Endnotes

1. TEX. RULES OF PROF'L CONDUCT R. 101 cmt. 8 (2019) (emphasis added).
2. See Peter Blumberg, *Facebook Vows to Improve Security After Hack of 29 Million Uses*, BLOOMBERG (Feb. 8, 2020, 9:42 a.m.), <https://www.bloomberg.com/news/articles/2020-02-08/facebook-vows-to-improve-security-after-hack-of-29-million-users>.