# Creating effective passwords

As an attorney, you have a professional responsibility to safeguard information entrusted to you by your clients. But if you or your staff are operating your office systems with weak passwords, you may as well open the door and invite hackers into your office files. Sufficient password practices are crucial to the implementation of effective cybersecurity practices. This article will provide you with a few tips for maintaining password policies that get the job done for you and your clients.

Every year, security professionals review data breaches to determine the most commonly used passwords. Surprisingly, or maybe not so surprisingly, a large percentage of people still use predictable and easy-to-guess passwords to protect even the most valuable data. Here are some of the most common for 2016, as listed by The Telegraph:

- 123456
- QWERTY
- 111111
- 123123
- Password
- 1q2w3e4r
- ZXCVB

If your go-to password is included on this list, you have some serious work to do. You should also count yourself among this hall of shame if your password consists of your name, family name, birthdate, or social security number. These are all bad ideas that can make your accounts vulnerable to hackers and thieves.

Your password works similarly to your office door keys. It serves as a barrier, locking unwanted individuals out of your files and confidential data. There are numerous steps you can take to improve the cybersecurity of your practice. For example, many law firms are moving from antiquated storage procedures to cloud-based systems.  While this is an excellent step

in the right direction. a good password system is still one of the simplest and quickest steps you can take right now to increase the security of your legal office.

## Choosing passwords

It sounds like a simple task, but choosing a strong password does take a little time and effort. You need to create a combination of letters, numbers and symbols that is difficult to guess, with essentially little meaning. Yet, it must be a combination that you can etch into your memory. It's a tall order to fill, isn't it? Especially if your memory tends to fail you from time to time. You might find yourself constantly having to change your password or embarrassingly locked out of your accounts… again.

I scoured the internet for help with this necessary task and here is a list of some tips I found:

- Don't use words found in the dictionary. These words are more easily identifiable to computer hacking programs.
- Create a sentence that describes yourself and then use the first letter of each word. For example, the sentence "My favorite color is green" translates into the following password: MFCIG. You can then add numbers and/or symbols to this base password.
- Try to use at least 10 characters (in fact, 10 characters is the mininum when creating a password in TimeSolv)
- Use different passwords on differents platforms. A simple way to do this is to insert the platform into your base password. For our MFCIG example from above, you could use MGOOGLEFCIG for your Google account and MBILLINGFCIG for your law firm billing software
- Use a password management program. These systems help you create strong passwords and provide reminders when it's time to change them.
- Change your passwords every 3 to 4 months.

Also, each member of your staff should have his or her own password. Sharing passwords can severely compromise the effectiveness of your

security system, so take the time to ensure that every person utilizes a strong and distinct password.

---

**About Erika Winston:**

*Erika Winston is a freelance writer with a passion for law. Through her business, The Legal Writing Studio, she helps legal professionals deliver effective written messages. Erika is a regular contributor to TimeSolv and a variety of other publications.*