



# Keeping your passwords strong and secure

Computer passwords are the keys that “unlock” our computer and network systems. We all have more passwords than we can remember. This tends to make us a bit lazy. We use obvious and easy-to-remember passwords – even the word “password” itself. Or worse: we don’t use them at all. Bad password habits are often one of the weakest links in data security schemes. Cyber criminals know and exploit this fact.

For this reason it is critical that all lawyers and staff in a law office use passwords, and use them properly. This article reviews the steps you need to take to protect the confidentiality of your passwords, and how you can create passwords that are harder to guess or determine.

 Many of the password best practices mentioned in this article are very easy to implement – review them with your lawyers and staff.

## Can you keep a secret?

Passwords don’t work if they aren’t secret. Unfortunately, people get careless and don’t always keep their passwords confidential. These are the things you can do to keep your passwords secret.

**Never ever tell anyone your passwords:** This includes your IS support person (they can force a reset if they really need to access your account). And, make sure no one is looking over your shoulder when you are typing a password. If more than one person knows about a password, it isn’t a secret anymore.

**Never write down your passwords, especially on your monitor:** Is this not the same as leaving the keys for your car in the ignition? Take a walk around your office and see how many passwords you can find on little notes taped to monitors or keyboards. If you absolutely have to write down some of your passwords to remember them, don’t write them out exactly. Write without an obvious reference to the account they apply to, and so they have to be translated in some way. Add or delete a character, transpose letters, or vary them some other consistent way which only you can figure out.

**Don’t save passwords on your computer hard drive:** It is not uncommon for people to create a document with all their passwords in it on their computer. This file can be located in seconds with a hard drive search, especially if it is called password.doc or if it contains the word “password” or other related terms like “username.”

**Use a password manager:** If you must store passwords on your computer or smartphone, use a password manager. These handy programs remember and enter passwords for you and they are stored in an encrypted form so that they can’t easily be accessed. Widely used password managers include 1Password, LastPass, and RoboForm. Some password managers let you sync and use your passwords on multiple platforms and devices across the web. Very convenient, but depending on your personal preference and the work you do, you may want to be cautious about putting your passwords in the cloud. Make your password manager password extra complex! (And make sure you don’t forget it.)

**Use biometric scanners:** Some laptops and the most recent iPhone have built-in biometric scanners that give you access to a device or other logins with a swipe of your finger or by facial recognition. These scanners help you avoid the need to remember passwords.

**Don’t use the same password for everything:** This is very tempting, but is also very dangerous as anyone that figures out your password can get easy and instant access to all your other accounts. Use a unique password for each program, especially for very sensitive things like your network logon, remote access to networks or bank account logons. You also shouldn’t use the same passwords for home and work purposes or on the administrator and user profiles on the same computer.

**Change passwords on important accounts on a regular basis:** For critical things like your computer and bank account, you should change your password every 60 to 90 days. This will foil a lurking hacker that has your password unbeknownst to you.

**Change any compromised password immediately:** Do this even if you only suspect a password has been compromised. Again, this is to foil a lurking hacker.

**Don't use the "remember password" feature:** Be wary of dialog boxes that present you with an option to save or remember your password. These can appear in your web browser and for remote access. By selecting this option you give unchallenged access to accounts to anyone sitting down at your computer.

### Use two-step authentication

Using two-step authentication on sites that offer it will help to increase the security of your online information. Two-step authentication is a process involving two stages to verify the identity of someone trying to access online services.

You are already using two-step authentication if you withdraw money from an ATM. To access an ATM, you need two things: the ATM card and a personal identification number or PIN. If you lose your ATM card, your money is still safe; anyone who finds the card cannot withdraw money if they do not know your PIN. The same is true if someone knows your PIN and does not have the card. This second layer of security is what makes two-step authentication more secure.

More and more websites are offering two-step authentication, including Google, Facebook, Apple, Dropbox, Twitter, Microsoft, Amazon, Evernote, WordPress and Yahoo! Mail. You should enable two-step authentication if you are using one of these services.

Many of these sites have also added a feature that notifies you by email or text message if your configuration has been changed. In some cases you have to confirm the change for it to remain in effect. This protects you in the event a hacker gets into your account. If the hacker changes your password or other settings on the account, you get an email or text message notifying you of the change and you have the ability to prevent it from happening. Enabling this feature on any of your accounts that have it will help prevent those accounts from being taken over by a hacker.

### Creating "strong" passwords

When you pick a password, you can't just use any password. It shouldn't be anything obvious and easy to guess, either by a human or a computer. Password-cracking tools continue to improve and they use one of three approaches: intelligent guessing, dictionary attacks and automation.

Intelligent guessing involves using words, phrases and key combinations that people commonly use as passwords. Intelligent guessing works reasonably well because most people use simple and obvious passwords (e.g., password, 12345, qwert, etc.). Dictionary attacks cycle through a complete list of words from one or more languages. Automated (or "brute force") attacks try every possible combination

of letter, numbers and other characters. Given enough time, the automated method can crack any password. The computers we have today are much more powerful so passwords that used to take months to crack can now be cracked in days or hours.

So, your challenge is picking a password that is hard to break because it isn't short, obvious or a common word. This is called a "strong" password. For a password to be strong it should:

- Not contain your name or your computer user name;
- Not be a word associated with you (e.g., your spouse or child's name, street name, etc.)
- Not be a common word, name or phrase;
- Be significantly different from any passwords you have used previously;
- Be at least 12 characters long, and longer is even better;
- Have at least one symbol character in a position other than the first and last;
- Contain at least one character from each of the following four groups:
  - a. uppercase letters A, B, C, ...
  - b. lowercase letters a, b, c, ...
  - c. numerals 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
  - d. symbols (all characters not defined as letters or numerals, including: ` ~ ! @ # \$ % ^ & \* ( ) \_ + - = { } | [ ] \ : " ; ' < > ? , . /

The best practice is to create a unique, complex and random password for every service you use. There are online tools that will create passwords with totally random characters. While these will be stronger, you will likely have to use a password manager to remember them.

### Passphrases can help you remember complex passwords

If you follow the advice in the previous section, your password will be an unreadable mix of letters, numbers and characters. While good for security, they will be hard to remember. Consider using a "passphrase" to remember complex passwords. A passphrase is a mix of letters, numbers and characters that has a translation that makes it easier for you to remember the correct sequence. Here are some sample passphrases:

- !am@#1DJ!nuSSr "I'm a number one DJ in Russia"
- Rm@j0risKrayz "Our major is crazy"
- l@wPR0!sgr8! "LAWPRO is great!"

Using strong passwords can help you better protect the confidentiality of client and firm data and systems. Encourage everyone at your firm to make sure all their passwords are strong and secure. ■

Dan Pinnington is vice president, claims prevention and stakeholder relations at LAWPRO.



QUICK  
FIX