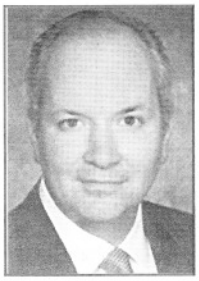

Smart Lawyers, Dumb Passwords

By Christopher Hopkins, Chair,
Law Practice Technology Committee

I bet I can figure out the passwords you use on the Internet. I say "passwords," plural, assuming you actually use more than one for different accounts. Does the password on your work computer use the firm name or initials? Do you use your spouse's, children's or pets' names? In light of recent *Florida Bar News* stories, lawyers are still falling for *Catch Me If You Can*-era scams. If you have responded to emails from African royalty or strangers with money held up in Asia, I am going to guess your secret password is… "password."

Statistically speaking, I would probably guess correctly in a few dozen attempts. Nearly 80% of us employ personal information or phrases in our "secret" passwords. http://bit.ly/gVjX2H According to a study of 32 million recently leaked passwords, 50% of people use names, slang, dictionary words, consecutive digits or adjacent keyboard keys as passwords. http://bit.ly/i27vJH In another study, 26% of users recycle the same password for different important accounts (e.g., email and bank). http://bit.ly/eklBtn Likewise, 75% of people use their email password as their Facebook and Twitter passwords. http://bit.ly/enZZpy One study compared password techniques in 1990 to current day and found… people have not updated their poor methods. http://bit.ly/ebpSa4 Microsoft studied a half-million people and revealed that users often had 30 or more accounts but simply re-used the same five or six (weak) passwords – worse, even with simple, repeated passwords, 4% of Yahoo Mail users forgot their password over a 90 day period. http://bit.ly/hAM9Hn In short, cracking one weak password will likely leave other accounts open for exploitation.

Lawyers need to protect themselves more than the average user. You have client information to protect as well as your own. Your job makes you more "visible" and, as evidenced by the Bar News articles, someone obviously decided that Florida lawyers are easy targets.

Lawyers routinely make careless mistakes with their security. Many of us leave our work computer on most of the time – even overnight – not realizing the exposure caused by your Internet browser, which you dutifully trained to auto-complete passwords. Simply double-clicking Explorer would give anyone access to your Internet accounts. A lost smart phone could be a security disaster. Depending upon the amount of office support you have, there are likely secretaries, paralegals, and even other lawyers who likely have some of your passwords (I once worked for a lawyer who gave me his PC password: "money").

Worse, crib notes of passwords are taped to computers; saved in Word files or Outlook emails frankly entitled "passwords"; or the secret list may reside on your smartphone which is not password-protected. Anyone who has access to your office in your absence could find a trove of information in under fifteen minutes (remember the Russian spy ring busted last summer? Despite high-tech espionage tricks, they wrote down their encryption password, http://bit.ly/ekwh3d). The best encryption techniques still succumb to human memory and our lazy practices.

In the last year, two high-traffic Internet sites (Gawker.com and Rockyou.com) were hacked and millions of passwords bled out to the Internet. The *Wall Street Journal* scoured the list to reveal the most common passwords: 123456, password, loveyou, f***you, QWERTY, and computer. http://on.wsj.com/e5ypES Even snarky passwords appeared to be commonplace: "trustno1" and "letmein" were among the top 20 passwords.

This should not suggest that you must turn to 256-bit symmetric algorithms to lock down your accounts. Computer professionals generally agree that even the best security can be beaten. I am going to assume that, if a lawyer is "targeted" by computer specialists, accounts will be hacked. Shore up your security at its weakest link – you – to avoid opening yourself to scams, disgruntled employees, and thieves. Simply stated, careless and downright silly Internet security practices need to come to an end.

First, if you use a password list or registry, make sure it is password protected on your smart phone or in a locked Word document (again, these are not iron-clad security methods but should eliminate opportunity crime).

Second, turn to the password policy used by rocket scientists at NASA (http://bit.ly/fHf8ny):

* use eight-character passwords at a minimum;
* mix UPPER, lower, numeric, and special characters (the latter should not be at the beginning or end (e.g., password@) but avoid "passw0rd" or "p@ssword");
* do not use a name or slang/dictionary words.

Third, consider these password guidelines:

* do not use pet names, high school, hometowns, and birthdays which are either public record or can be obtained from Spokeo.com or social media sites – also avoid these as password reminders and hints;
* avoid repeated (11111), consecutive (12324), and adjacent (QWERTY) character passwords;
* change passwords routinely;
* consider programs like KeePass, RoboForm, LastPass, and TrueCrypt;
* hackers will use programs which test every word in the dictionary (starting with the commonly-used passwords, above) in "brute force" attacks which are often stymied by combining "numer1c" and "speci@l" characters;
* use a base password (like "ASDF") and then customize it for different sites (ASDF@ebay) or use other memory tricks (http://lifehac.kr/e4TeMC);
* consider using a website address as a password to confuse a key-logger attack;
* password-protect your computer (notably, Windows allows a space as a password character) and your smartphone.

Lawyers know and (often) exceed standards to keep client information confidential. Simply having a password – particularly one that is obvious, common or accessible – is not enough. Make sure your personal and professional information is likewise secure.

Christopher Hopkins is a shareholder at Akerman Senterfitt and is the Chair of the Law Practice Technology Committee. Tape a "X" to your front window or email him at christopher.hopkins@akerman.com