Password Protection

A June 2011 discussion on SoloSez, the email listserv for general practice, solo and small firm lawyers

I am inquiring as to how others handle the myriad of programs and devices requiring passwords. Not only are the passwords supposed to be random letters and numbers, but they are supposed to be frequently changed. How and wear does one store all the different passwords. Surely you don't store them on your computer; that would be tantamount to storing the key to your car in the tire well (which I don't do). Maintaining a manual file seems so 20th century. Perhaps I am memory challenged and can't remember one password, much less a dozen.

Lastpass.com

Dave Rakowski, Pennsylvania

My friends over at Paradigm Computer Consulting just posted a blog about one method of coming up with passwords that sounded pretty interesting. Perhaps it could work for you.

http://www.paradigmcomputer.com/blog/item/12-how-to-choose-very-strong-passwords-that-are-easy-to-remember

Nancy Duhon, Georgia

There are several password programs out there that handle this issue. You just need to remember one main PW and the software generates a PW for whatever site or program you need. Look at LastPass, Keepass, Roboform, etc. I am sure there are others. Google password management software. Some are free; all are very reasonably priced if not free.

Dennis Riley, Illinois

For online passwords I use a free service called LastPass that I think stores passwords in the cloud and on the computer in an encrypted state. Still have to remember at least one password to use.

Easy to setup and use.

Glenn A Brown, Pennsylvania

I actually do have a chart on my computer where I have a list of my usernames and passwords, but only the ones that I don't use on a daily basis, because some (like my banking site passwords) are in my brain, and others (like LinkedIn) I don't use every day so I can't remember them.

Anna D. Collins Ford, Paralegal

I am a big fan of KeePass, which I use on my Windows and Linux systems. I use a combined master password and key files, with a master copy of the keys stored on a flash drive in my office safe and a "day-to-day" copy for home/office use. See http://keepass.info/index.html for more information.

Lorraine Harrington, Arizona

I use lastpass.com and have for a couple of years. It works beautifully. They recently purchased Xmarks, which is a bookmark storing/syncing utility, so you can get both password storage and bookmark storage with lastpass. They also make an app for just about every type of device.

Nanette J. Gould, Tennessee

I have hundreds of passwords, and I store them in a spreadsheet that is password protected. After setting up the spreadsheet, I also modified it so that the rows for the password do not line up with the rows for the user ID. Those rows area offset by a number of rows that I only know.

There are commercially available programs for password storage and retrieval.

I realize that a sophisticated hacker can probably break the password for my spreadsheet, but I would also think the sophisticated hacker can break into the protection scheme of the commercial software.

Gerald Hoenig

I've used Roboform for several years. I love it, though I've never fully used the sync function, where I supposedly can access my passwords anywhere

Patrick W. Begos, Connecticut

I use LastPass.

I would like the techie folks to weigh in with an opinion as to whether they think password managers are safe.

FYI LastPass did have a "security incident" last month:

Subject: LastPass Security Incident #4dc8f7ceada02 Date: Tue, 10 May 2011 08:31:11 +0000

Dear LastPass User,

On May 3rd, we discovered suspicious network activity on the LastPass internal network. After investigating, we determined that it was possible that a limited amount of data was accessed. All LastPass accounts were quickly locked down, preventing access from unknown locations. We then announced our findings and course of action on our blogand spoke with the media.

As you know, LastPass does not have access to your master password or your confidential data. To further secure your account, LastPass now requires you to verify your identity when logging in. You will be prompted to validate your email if you try to log in from a new location. This prompt will continue to appear until you change your master password or indicate that you are comfortable with the strength of your master password.

Please visit https://lastpass.com/status for more information.

Thanks, The LastPass Team

Thanks!

James H. Pardue, , North Carolina

The Lifehacker blog has a good rundown of five different password manager programs, here . I've generally found Lifehacker's advice and information to be pretty helpful and reliable. The commenter community there is also very tech-savvy, and often helpful.

Some of the points Lifehacker makes in favor of KeePass (which, coincidentally, I just started using a couple of days ago), are that it's open-source, so ostensibly more secure, as well as being free, and it includes a built-in password generator to create extra-secure alphanumeric passwords. You also can set passwords to expire after a certain time, at which point I think the program will prompt you to change them -- keeps you from becoming complacent. The article above also links to some further articles about maximizing your use of KeePass.

Overall, the idea seems to be that your information is much more likely to be compromised by an online hacker, than by someone who accesses the data directly from your computer or a backup flash drive. There's no way to eliminate the risk completely, but using a set of changing, strong passwords seems to be an important step.

And, since this is my first post, I suppose I should introduce myself. My name's Emily Wendel, and I just graduated a few weeks ago from the University of Toledo College of Law (although the J.D. has yet to land in my hot little hands). I'm a candidate for the 2011 Ohio bar exam. My favorite drink is a gin and tonic (Tanqueray Rangpur is particularly nice), and I don't have any pets right now, although I'm soon going to be adopting my mother's 20-pound Maine Coon mix cat, named Scamper. When he's not being adorable, he likes to climb on you while you're sleeping and give you a nose piercing.

Nice to meet you all! Rob Switzer referred me, since I'm new to the field, and I'm considering going solo once I'm licensed.

And now the obligatory statement, I am not a lawyer, and I don't give legal advice. If you want legal advice, hire a lawyer.

Emily E. Wendel Juris Doctor Candidate, May 2011

There are people that are a more offensive on twitter; of course, those are generally anonymous accounts.

Ive been using KeePass for about 4 years. I sync it across my Mac, iOS, and Ubuntu installs. Its sick. There is simply nothing else that does what it does, as well as it does, across every OS youre likely to use.

The best advice Ive ever received about passwords is from a client of mine. He uses an algorithm for every site. Not his suggestion, but lets say you want a password for amazon, youd take the first and last letters a and n and use those to surround a passphrase that incorporates some number derived from amazon, maybe the number of characters in the TLD. So, if the phrase is bite[number of characters in TLD]me, the amazon password would be abite6men. Its easy to remember the algorithm, but quite difficult to uncover the algorithm is a password or two is jacked.

Steve O'Donnell, Pennsylvania

The major concern in my mind is using the same password across different sites. If one site is compromised, the person would have access to any number of your other accounts.

What if someone got into your Twitter account and jacked it up or posted crazy things posing as you? Crazier things than you'd normally post. :) The same thing for Facebook, Gmail, etc.

You may not lose anything of true value except time fixing the damage, but it's still something I'd rather avoid.

That's KeePass's true value. I only know about 3 of my hundreds of random passwords. If I get a notice that a site had a "security issue," I just change that one password.

Andrew Flusche, Virginia

OK I understand the worry about using the same password across sites and it is a valid concern. But you chose a bad example. Someone posting crazier things than Steve O on Twitter??? Really?

Dennis Riley, Illinois