Password managers: Security made convenient

Levi King

kingle@metrostate.edu

Give this a try. Count, on your fingers, how many passwords you have to remember.

This exercise tends to divide people into two groups. Either you can't do it because you have too many accounts, or you can do it ... but only because you reuse the same password for multiple accounts. Either way, you have a security problem.

Last month we covered Two-Factor Authentication, or 2FA, a simple way to improve your security using your phone. You might remember I laid out three rules for good password security: don’t share them, don’t reuse them and don’t make them easy to guess.

This isn’t always easy! Sometimes we share passwords for shared accounts, like a household subscription. Other times we’re too lazy to make new passwords for new accounts. Often we make them too simple, like a pet’s name. (Come on, anyone could find that on your Facebook!)

**Get a Vault**

Fortunately, there are programs designed to save us from our security laziness. They’re called password managers, and they give you the best of both worlds. A password manager stores your long, complicated, and secure codes for all of your accounts, in a virtual “vault” for safekeeping.

You might ask: how does putting all my passwords in one program make me more secure? Couldn’t I accomplish the same thing by putting them in an encrypted document? Well, you could, and it would be better than taping them under your keyboard. But what if you don’t have a device that can open the document handy? What if the document gets deleted?

The most important thing password managers do is make security convenient. They can generate new, better passwords for all your accounts and automatically type them so you don’t have to go searching for the key on your phone keyboard. They can use one-time passwords to keep your account secure if somebody recorded your keystrokes on a public computer. They can even share passwords to multiple people and sync changes for easy access. In short, they solve all your password problems.

**Where Do I Start?**

First, pick one! There are many options: KeePass, Dashlane, 1Password, RoboForm, and more. Personally, I use LastPass. Most have basic free versions (KeePass is totally free), and even the paid ones aren’t pricey. For example, $1/month for LastPass gets you an app for your phone, fingerprint scanner support, and other 2FA options.

Second, pick a good, long password (something you won’t mind typing frequently) and install your chosen manager. Some are no more than a desktop application to copy/paste the passwords from, while others can automatically fill in password fields in your browser.

Third, start logging in! You don’t need to get every account done in one sitting, because you’ll get feedback as you go; when the manager detects a weak password, it can suggest a switch to a longer one. In my case, LastPass has something called a “Security Challenge.” It scans the vault for weak passwords and checks a list of recently hacked websites for more that might need updating. This helps me stay on top of my personal security.

At the end of the day, there are a few passwords you can’t afford to forget. Your phone needs an unlock code, ATMs need PINs, and classroom computers need your StarID. It’s not about logging you in automatically everywhere you go (because we haven’t got biometrics like fingerprint scanners all over the place just yet); it’s about reducing your mental workload by handling the basic security stuff automatically. Don’t put this off until something gets hacked!