Password Managers

What is it?

A password manager, or vault, is a place to securely store and recall your passwords. In addition to storing and remembering passwords, password managers also make the authentication process easier to use. Depending on the product you choose, you can drag and drop your passwords into the web form, or the manager will recognize the service provider and auto-fill your credentials. In other words, you may never have to type a password again.

Some password managers allow you to store additional information with each password, like answers to those annoying security questions. Yes, you never again have to remember the answers to those questions. Even better, you can create answers that are pure nonsense because you don’t have to rely on your past to remember them. This makes them more secure because they’re no longer guessable based on personal information that’s publicly available (e.g., pet’s name, high school mascot).

The only thing you have to remember is the password you set to protect access to your manager.

Why should I bother?

Passwords by themselves are no longer considered a secure and private form of authentication. In the past few years, literally hundreds of millions of commonly used passwords have been exposed\(^1\) and published on the Internet.

This enormous repository of passwords is mined by cyber gangs who meticulously test the credentials against the major on-line service providers (Gmail, Hotmail, Facebook, Twitter, Instagram, banks, etc.) to find valid matches that give them access to active accounts.

Since many people reuse the same password, or slight variations, for multiple service providers, the chances of finding a valid match are relatively high. This is why you should use a password manager: so you can use a unique password or passphrase for every service provider.

Sample Password Managers

Keepass

Keepass is a local password manager. The encrypted database containing your passwords is stored on your hard drive, or a USB stick. It has to be physically present to access the stored information. Here’s a screen shot of an entry.

---

\(^1\) https://haveibeenpwned.com/Passwords

Information Technology Services

albany.edu/its
This record is for a Hilton Honors account. Double clicking the URL field will open the site in your browser. At that point, you can drag and drop the User Name and Password into the web form. It’s that easy.

**LastPass**

LastPass is a cloud based manager. It requires a browser plug-in. The advantage is you don’t have to tote your password file around to have access to it. The disadvantage is you’re trusting the cloud provider to secure your Internet keys. With LastPass you access your sites from your “vault” via the browser plug-in.

As is the case with Keepass, you just click on the saved site with the stored credentials to open the web form. LastPass will automatically fill in your User Name/Password combination and initiate authentication.

**Other Options and Disclaimer**

These are just two examples of password management products. An on-line search will reveal more. In fact, searching on “password manager reviews” will provide you with many more options that have been independently evaluated.

The University at Albany does not endorse any particular password management product, and those cited here have been selected solely to provide examples of storage options (local and web) and standard features.