

## Password Managers

April, 2014



One of the most frequent challenges I hear about from my customers is how to deal with passwords. In past newsletters I have covered how to create strong passwords that are unique for each website, but I must confess, password management can still be unwieldy. Personally, across all my email accounts, banking and financial accounts, websites I purchase from, social websites, and my wife's accounts, I have over 75 passwords that I have to keep track of.

To help manage this mess, I recently started researching password managers. There are many choices out there, including Lastpass, Dashlane, RoboForm, 1Password, Keeper, Norton Identify Safe, KeePass, and CommonKey. In my case, I wanted something that was either free or very low cost, covered Windows, Mac, iPhone, and iPad, supported all the common web browsers including Internet Explorer, Google Chrome, Mozilla Firefox, and Mac Safari, and was very secure.

Fundamentally, all the password managers work by establishing a master password that must be entered to gain access to your database of passwords. Therefore, your master password must be a really strong one. Theoretically, other than your master password, you do not need to remember your other passwords. Most of the password managers will even create a random password for you, relieving you of the challenge of creating and remembering great passwords. Heavy use of encryption and other security techniques should prevent others from ever being able to get access to your passwords. As you log on to your existing accounts, many of the password managers will take note of your id and password and store them for you, giving you the option to automatically log on in the future. Quite a few of them allow you to log into your store of passwords via the web so that they can be used from other people's computers. The passwords are stored encrypted and only decrypted locally on your device. In this way, even if someone breaks into the

LastPass servers, they will not be able to do anything with the encrypted passwords. These are just the basic features; there are many more beyond this foundation. I have been playing with the most recent version of LastPass, which meets all my requirements. So far, I like it. It is free for desktop computers (Windows and Mac) and for the very low price of \$1.00 a month, you can also use it on all your mobile devices. One thing I'm not thrilled about is that on the Apple mobile devices, LastPass provides it's own web browser. This is because Apple has not opened up a third party interface for Safari, giving vendors like LastPass no choice but to provide their own.

LastPass does take some effort to set up (be sure you install what they call the binary version) and some web sites require extra effort to get LastPass to work just right (in particular auto login does not work on all sites). If you are going to install and configure LastPass yourself, I recommend you first read the manual, then install it on your favorite browser and try it on just a few web sites before committing to it wholeheartedly. As part of setting it up, you should also think about your current passwords and if they are not strong passwords, take the opportunity to change them. If you do commit to LastPass, you can import all the passwords that your web browser has been saving for you, after which you should delete them from your web browser and change its setting to no longer save them.

I have resisted password managers for a long time, but given the diversity of my accounts and passwords, plus the probability that web sites will likely begin to require frequent password changes, and security breaches such as the recent Heartbleed bug, I'm ready to commit to it. You probably should too.

You can check out LastPass at [www.lastpass.com](http://www.lastpass.com).

*As always, I hope you have found this information useful. If you do not wish to receive these emails in the future, let me know.*

*This newsletter, as well as all past newsletters, can be found on my web site (<http://steve.gimnicher.com>).*