Tech Coach Corner – Password Manager? We Don't Need No Stinking Password Manager (Part 2)

I hope you've read Part 1 where I discuss what a password manager (PM) is and why you need one. If not, I recommend you go back and have a quick look. If I have not convinced you that you do need a PM, then don't waste your time reading the rest of this article.

Decisions, decisions, decisions

If you live totally in the world of Apple, then the iOS Keychain can be a good option. It's free and part of your operating system. Overall, iCloud Keychain is a competent password manager — but it is missing other features that third-party password managers provide.

If you don't live in Apple-world or decide to move beyond iOS Keychain, you have an almost overwhelming choice of options, as shown in the table below. Remain calm and keep reading; I won't explain every feature (left-most column) in-depth, nor will I take you through each PM listed. Rather, I propose to use this table to help you identify what features might be important to you. Before we start, however, please do familiarize yourself with the text table under the graphic (*Explanation of attributes and terms)* so you can follow the discussion. In addition, I'll focus on places where blue checkmarks are missing, as those might be features that you want. OK? Let's go on this short and easy ride.

Autofill Form is one of the most useful of features. I would exclude KeePass on that basis alone, except for one other feature – it is one of the best **completely free** PMs available.

Security Alert is missing from most of the PM, and you might wonder why. My answer is that the antivirus on your computer (What? You don't have one? Oh my.) serves that purpose. If you don't have an antivirus program, you need one – immediately if not sooner. Even Apple products are hacked!

Single Sign-On (SSO) is important only in the corporate world; even though my PM has it, I do not use it.

On-Premise and Cloud Based are pretty much mirror images of each other; the former stores your passwords **only locally** (on your device). The disadvantage of this security is that you must remember to load your passwords onto all devices whenever you make a change. Cloud Based means your passwords are accessible wherever you are (I can retrieve mine while traveling in Europe, for example). The downside is risk of the cloud being hacked. I use multiple devices, and for me the security of on-premise isn't worthwhile.

Assuming I've covered the features that are important to you, how do you choose among these riches? Cost is always a good way – most commentators agree that **Lastpass** is the best of the freebies. Here's why: most other free PMs limit you to a single device if you don't pay up. While some of the others in the table have a free option, they will generally limit you to a single device unless you pay up.   [LastPass](#) stands out as the best free PM by giving you the ability to store passwords, user login info and credentials, and synchronize all of it wherever you want -- across desktop and mobile devices and browsers.   Paying will get you some additional features, but they aren't critical.
If you want to go beyond free, then it will come down to cost. While most of the PM companies will provide a free trial version, those versions might not have all the features and will expire after a defined period. This isn't like buying a car, where a test drive is necessary. You are best off picking one and sticking with it. RoboForm is among the oldest of the PMs, probably has the largest user base, and is among the least expensive ($1.98 to $3.98 per month – single vs. family plan). Prices for others are higher, although none exceed $5.00 per month currently). I've been using it for more than 15 years and it provides me everything I need, and more. (Disclaimer: I do not work for the company nor am I paid to recommend it.) It doesn't have the prettiest interface (that award probably goes to Dashlane), and a peculiar downside is that it has more features than you will ever use), but it has excellent online help and good customer service.

	Lastpass	KeePass	1Password	Dashlane	Passwordstate	Keeper	Sticky Password	Devolutions Password Server	RoboForm
Offline Mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
Two-Factor Authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓
Browser Integration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Autofill Forms	✓		✓	✓	✓	✓	✓	✓	✓
Password Generator	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security Alert	✓		✓	✓				✓	
Portable Application	✓	✓		✓		✓	✓		✓
Mobile Application	✓	✓	✓	✓	✓	✓	✓		✓
Security Audits	✓		✓	✓	✓	✓		✓	✓
Import Passwords	✓	✓	✓	✓	✓	✓	✓	✓	✓
Export Password	✓	✓	✓	✓	✓	✓	✓	✓	✓
Single Sign-On (SSO)	✓					✓		✓	✓
Password Sharing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Integrated Database	✓		✓	✓	✓	✓	✓	✓	✓
On-Premise		✓	✓		✓	✓		✓	
Cloud Based	✓		✓	✓		✓	✓		✓

Source: https://blog.devolutions.net/2019/01/updated-2019-most-popular-password-managers-compared

Explanation of attributes and terms

Offline mode	Functions without being connected to the Internet
Two-factor authentication	Allows you to need both a password and a security code that is mailed/texted upon request
Browser integration	Integrates with web browser
Password generator	Generates a new password when you request
Security alert	Alerts you if someone tried to hack into your account
Portable application	Works with portable device (laptop or tablet)
Mobile application	Works with mobile (smartphone)
Security audits	Will examine your device for security issues
Import passwords	Import passwords from another application
Export passwords	Export passwords to another application
Single sign-on (SSO)	One sign-on gains access to multiple processes (only important in the corporate world)
Password sharing	Means just what it says…and should **never** be done
Integrated database	Integrates data from several sources (only important in the corporate world)
On-premise	Passwords stored locally (on your device)
Cloud based	Passwords stored in the cloud (accessible from wherever you are)

If you have any specific questions about this, please feel free to contact LTCL Tech Coaches at techcoach@laketravislibrary.org and one of our coaches will respond.