Serials Review

Routledge
Taylor & Francis Group

ISSN: 0098-7913 (Print) 1879-095X (Online) Journal homepage: https://www.tandfonline.com/loi/usrv20

Choosing the Right Password Manager

Elizabeth A. Gallagher (Contributor)

To cite this article: Elizabeth A. Gallagher (Contributor) (2019) Choosing the Right Password Manager, Serials Review, 45:1-2, 84-87, DOI: 10.1080/00987913.2019.1611310

To link to this article: https://doi.org/10.1080/00987913.2019.1611310

Published online: 21 May 2019.

SERIALS REVIEW
2019, VOL. 45, NOS. 1–2, 84–87
https://doi.org/10.1080/00987913.2019.1611310

Routledge
Taylor & Francis Group

SHARPEST TOOL IN THE SHED: ELYSSA M. GOULD, COLUMN EDITOR

Choosing the Right Password Manager

Elizabeth A. Gallagher, Contributor

University of Tennessee Libraries, Knoxville, Tennessee, USA

ABSTRACT
This segment of the Sharpest Tool in the Shed column explores three password manager options to consider incorporating into your library. Many libraries and businesses still rely on an Excel spreadsheet to house the myriad log-ins and passwords that staff need to do their daily work. Choosing the right password manager can save staff time and enhance security. This segment draws on research and trial experiences of three popular password managers: 1Password, LastPass, and KeePass.

KEYWORDS
1Password; KeePass; LastPass; memory; password manager; security

Introduction

It can be difficult to remember all of the log-ins and passwords we use to conduct our daily work. With so many passwords to remember, we typically forego creativity and choose passwords that are easily remembered or something of current interest. This is why "123456" and "password" always top the lists of worst passwords since 2011, and why "starwars" was in the top 20 used passwords for 2017 (Korosec, 2017). We need something quick and memorable. However, quick and memorable is exactly what hackers want. From millions of users' passwords being compromised—from Under Armour's fitness app to Iranian hackers stealing 31 terabytes of information that involved 144 U.S. universities—2018 alone has seen its fair share of data breaches (Newman, 2018). The potential for data breaches and compromised personal information increases when simple passwords are used across websites. Besides the lack of creativity in password creation, people also tend to store their passwords in vulnerable locations. It is common practice to store passwords in an Excel spreadsheet or on Post-it notes stuck to computer monitors, or the password is memorized by one individual who is planning to retire next month.

It is clear that this process is inefficient and not secure. So why do libraries continue to avoid password managers? One issue is shrinking library budgets. Most password manager plans have monthly fees per user. When budgets are tight, it is unlikely that funds can be allocated for better office management. Another issue is a misperceived lack of control over passwords within password managers. Users still fear the cloud, and it seems unsafe to put all passwords in one location. While password managers are not infallible (Fraunhofer Institute for Secure Information Technology, 2017), they are an extra credible security measure. As Emmanuel Schalit, CEO of password manager company Dashlane, stated, "Sometimes, it's better to put all your eggs in the same basket if that basket is more secure than the one you would be able to build on your own" (Nicholas, 2016). Post-it notes just won't cut it anymore.

Passwords and our memory

The human memory relies on familiarity and redundancy when it comes to password creation, making us vulnerable to attack. According to a study on creating secure passwords conducted by Lo (2016), people tend to use the same password with personal information tacked on. For example, adding a birthdate after the original password, or adding the current month when prompted to update a password. Human memory can hold about seven characters, so our memories simply cannot hold the long strings of random characters necessary to be considered secure in our online environment (Lo, 2016). A study conducted on 288 college students by Yan, Blackwell, Anderson, and Grant (2004) showed that adding personal attributes, like a birthday or pet's name, are useless against certain hacks. For example, if a hacker conducts a dictionary

CONTACT Elyssa M. Gould egould1@utk.edu Electronic Resources Librarian, University of Tennessee Libraries, 1015 Volunteer Boulevard, Knoxville, TN 37909.

attack, where the same word is used to populate possible passwords, then variations of a password are just as easy to hack (Yan et al., 2004).

Instead of relying on memory, people should harness the way human brains work to create memorable yet complicated passwords. Mnemonic phrases are just as strong as random passwords. Yan et al. (2004) explain, "An example of such a composition might be using the phrase 'It's 12 noon and I am hungry' to create the password 'I's12&Iah' which is hard for anyone else to guess but easy for you to remember." Hence, using a password manager can simplify your life. A user simply needs to memorize one mnemonic phrase that presents itself as random characters. The password manager will remember the rest, freeing up energy and brain power to work efficiently in your space.

How does a password manager work?

Password managers have been around for decades, but the overall process has remained the same (Mendelson, 1999). The user creates one complex password called a master key or master password. So instead of remembering countless log-ins and passwords, users simply remember their master key. Password managers do more than just house passwords though. They can also store secure notes, credit card numbers, and other important private information. Some also have security measures in place to inform you when a password has been compromised and prompt you to change weak or reused passwords. Password managers typically have a password generator as well. This feature can help create strong, secure passwords. Other features include browser extensions and two-factor authentication. It is up to the library to choose an appropriate password manager based on its needs. Factors to consider are price, security, support, quick setup, and easy maintenance. It is also important to know who will be using the password manager. Is it for individual use, a department, or all library faculty and staff? Varying levels of technological ability need to be taken into consideration as well. Luckily, there are many options for different price points and different technological abilities.

1Password

This author tried the 1Password (https://1password.com/) individual plan for one week. 1Password requires credit card information to be provided for the free trial. When creating an initial master password, 1Password also creates a "secret key" of random characters and a quick response (QR) code containing this information to set up the mobile app. Then there is the option to print or save this "Emergency Kit" information. This author needed her email address, secret key, and master password to set things up. After setup, the secret key is never used again unless users are locked out of their accounts. Setup took about 30 minutes, not including a comma-separated values (CSV) file import.

Browsing the 1Password "vault," where all the passwords are stored, was a bit bewildering at first. This author had never used a password manager before, and it seemed to come with some expectations for knowing how to navigate the vault. A tutorial or guide would have been helpful during the setup stage. There was also some trouble with the browser extension not working on the Chrome browser (https://www.google.com/chrome). This is probably due to the fact that all of the product's features do not work on Windows and Chrome (Kissell, 2018). A pop-up appeared and suggested uninstalling the plug-in and reinstalling it. Regardless of setup woes, 1Password's convenient features explain the ticket price. Password generator, two-factor authentication, mobile fingerprint recognition, browser extension, and security checks are all integrated into 1Password.

One feature of particular note was the Watchtower. Within the vault, Watchtower looked for breaches in security and checked information against haveibeenpwned.com (1Password, n.d.b). 1Password is used by many businesses, including CNN, BBC, Mashable, *The New York Times*, and NPR, with a price tag to match (1Password, n.d.a). The Team plan costs $3.99 per user per month, the Business plan costs $7.99 per user per month, and the Enterprise plan is a custom quote. Each plan can include any number of members, but each plan provides different features like added support and more storage per person. Those prices can add up quick when considering everyone in your department. Despite the price, 1Password is easy to use and has an extensive support page, blog, and social media presence. Most questions and concerns can be answered by viewing their Reddit page (https://www.reddit.com/r/1Password). Unfortunately, this author's emails to the support team about Excel spreadsheet imports remains unanswered to this day. For libraries that have the budget to devote to a password manager and time to appropriately train staff, 1Password can offer outstanding features to keep information secure and well managed.

LastPass

Second, this author tried a LastPass (https://www.lastpass.com/) individual plan for one week. No credit

Table 1. Password manager comparison table.

Password Manager	*Free*	*Exceptional Support*	*Easy Setup*	*2FA*	*Password Generator*	*Security Checks*	*Simple User Interface*	*Works Well on All Browsers*
1Password			X	X	X	X	X	
LastPass	X individual plan	X	X	X	X	X	X	X
KeePass	X	X			X	X		X

card information is required to get started on a free trial. All that is needed is a master password. After the trial ends, users can continue to utilize the free plan with all data remaining or switch to a premium plan for $2 a month for a single user. Keep in mind that the free option is only for a single user. There are more features on the premium plan, including "1GB of storage, an ad-free vault, and priority support" (LastPass, 2018). A team plan for five to 50 users is reasonable at $2.42 a month per user. The Enterprise plan for five or more users is $4 a month per user. Like 1Password, the more expensive plans offer more features.

After starting the trial and downloading the browser extension, LastPass walked this author through a user-friendly guided tour with pop-ups of explanations for specific tabs and where to find more information. It was exceptionally helpful. LastPass also offers extensive customer support with guides, videos, forums, and a support ticket page. A courteous response to a submitted support ticket regarding importing files arrived within the next business day. The browser extension worked well across different browsers, including Chrome, Firefox (https://www.mozilla.org/en-US/firefox/new), and Safari (https://support.apple.com/downloads/safari). The extension prompts the user to update weak or similar passwords to enhance security. Another security feature includes a security check that runs within the vault and provides a numeric score with suggestions for fixing issues. For about half the price of 1Password, LastPass is a great option for libraries on a budget that need a quick and easy-to-use password manager.

KeePass

This author tested KeePass (https://keepass.info/), an open source password manager, for one week. Download of the free software is available on SourceForge (2018) and takes about two minutes to install. The software is bare bones, like most open source software, but following the "First Steps Tutorial" provided in the KeePass Help Center is quite simple and user-friendly (2018). KeePass uses databases (their version of a vault) to store information. After making a database, users create a master password that can be printed off for storage in a secure location. KeePass offers several advanced options from file storage to pop-up reminders to update your master password. Passwords can easily be entered individually. Importing a CSV takes a bit more work, but help pages, examples, and file samples for a CSV or extensible markup language (XML) file import are available in the Help Center (KeePass, 2018).

Databases can be stored on a shared network for multiple users. Each user simply needs to use the master password for that database. Changes made within the shared network database will synchronize. A browser extension can also be utilized by each user to fill in log-ins and passwords directly from the shared database. KeeForm (2018), an open-source browser extension, works with KeePass to fill passwords on Firefox and Chrome. KeePass takes some time to understand and maintain, but a library willing to set up and train its employees can have a functioning password manager that works just as well as a paid subscription product without all the frills.

Conclusion

Password managers securely manage a multitude of secure information that our memories simply cannot hold. Each of the password managers explored here have something different to offer. Deciding which one to use is dependent on your users' needs. See Table 1 for an overview of the password managers reviewed in this article.

This author sees the password manager being used collaboratively by staff for work within technical services, such as serials management, electronic resources management, gathering usage reports, and downloading MARC records. The password manager could also be used cross-departmentally to securely share private business information throughout the library. In a large library, this might encompass a dozen people; in a small library, this might only be one to two people.

If it is for individual use, the free version of LastPass may be right for you. It offers an easy-to-use interface with amazing support without the price tag of 1Password. If using a password manager for a

department on a limited budget, taking the time to install KeePass may be the best bet. Again, open source software takes additional time for setup and training but works just as well. Whichever password manager you choose, it will save your library time and headaches while keeping your information secure.

References

1Password. (n.d.a). *1Password for business*. Retrieved from https://1password.com/business

1Password. (n.d.b). *1Password watchtower*. Retrieved from https://watchtower.1password.com

Fraunhofer Institute for Secure Information Technology. (2017). *Password manager apps [web page]*. Retrieved from https://team-sik.org/trent_portfolio/password-manager-apps

KeeForm. (2018). *A simple form filler for KeePass [website]*. Retrieved from https://keeform.org

KeePass. (2018). *Help center [website]*. Retrieved from https://keepass.info/help/base/index.html

Kissell, J. (2018). The best password manager. *Wirecutter*. Retrieved from https://thewirecutter.com/reviews/best-password-managers/.

Korosec, K. (2017). The 25 most common passwords of 2017 include 'Star Wars.' *Fortune.com*. Retrieved from http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom

LastPass. (2018). *Plans and pricing [web page]*. Retrieved from https://www.lastpass.com/pricing

Lo, C. (2016). Empirical study of secure password creation habit. *Lecture Notes in Computer Science*, *9744*, 189–197. doi:10.1007/978-3-319-39952-2_19

Mendelson, E. (1999). Keep the keys safe. *PC Magazine*, *18*(15), 134.

Newman, L. (2018). The worst cybersecurity breaches of 2018 so far. *Wired.com*. Retrieved from https://www.wired.com/story/2018-worst-hacks-so-far

Nicholas, M. (2016). *A skeptic's guide to password managers and security [blog post]*. Retrieved from https://blog.dashlane.com/a-skeptics-guide-to-password-managers-and-security

SourceForge. (2018). *KeePass download [web page]*. Retrieved from https://sourceforge.net/projects/keepass

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security and Privacy Magazine*, *2*(5), 25–31. doi: 10.1109/MSP.2004.81