The Navigator

A Financial Planning Resource from
Pekin Singer Strauss Asset Management



October 2018 | Issue 19

Password managers are digital vaults that help create and store passwords for online accounts and are an essential tool for ensuring your online security. Properly using a password manager can simplify your online life and, more importantly, make you less susceptible to problems like identify theft.

Why You Should Consider a Password Manager

by Josh Strauss, CFA & Erin Kelsey

Increasing Online Security with Password Managers

You probably have numerous online accounts on various websites, from your bank to social media sites to online retailers. Like many people, you probably also have difficulty keeping track of your various passwords for all those different websites, or you do not have passwords that are sufficiently secure. Password security is paramount for protecting your personal information against identity theft, but keeping track of all of your login information can be extremely challenging.

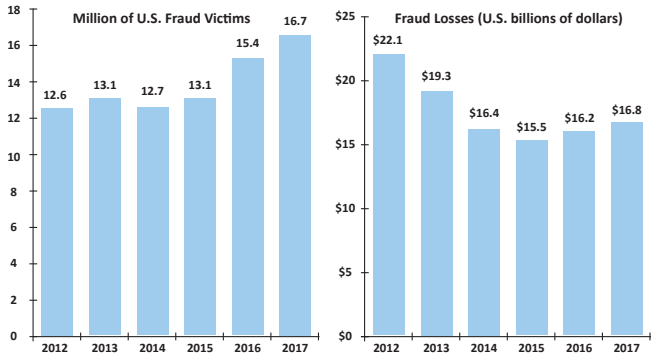
In this Navigator, we review an essential tool for helping you simplify your online life and increasing your security: password managers. Password managers are online services that create and store secure passwords for your online accounts, and their use both reduces the number of passwords you need to remember and makes your accounts less susceptible to hackers.

Why should I get a password manager?

In our previous Navigator, "The Growing Threat of Identity Theft," we discussed the increasing risk to consumers resulting from fraud. The annual number of victims of identity theft continues to rise, and identity thieves stole over $107 billion in 2017.[1] While most cases of identity theft are still due to stolen physical property, the Internet is a significant and fast-growing source of personal information for would-be thieves. Your online accounts can offer a fraudster a wealth of private data about yourself, and the increasing prevalence of hacks and data breaches makes securing your online accounts even more important. In fact, many home burglars are more interested in stealing your hard drive than your electronics or your jewelry; by accessing your hard drive, they can subsequently steal your identity.

Several of our recommendations in "The Growing Threat of Identity Theft" centered around increasing the security of your online accounts by using safer passwords, especially via the use of password managers. Security experts, consumer advocacy groups, and major publications all agree with this recommendation: password managers are an *essential* tool for increasing your online security. They are extremely

Fraud Victims & Losses Continue Three-Year Rise



Source: 2018 Identity Fraud Study, Javelin Strategy & Research

1 https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

Pekin Singer Strauss Asset Management

161 North Clark Street, Suite 2200, Chicago, IL 60601 | www.pekinsinger.com
312.554.7525 | 800.648.6361 | matt@pekinsinger.com

simple to use and make your online accounts much more secure, plus they provide peace of mind that your personal information is well protected.

While storing your information online is extremely convenient, you have probably also found yourself creating more and more online accounts over the past few years, and you are asked to create a unique password each time. The problem for consumers is that the most secure passwords are also the hardest to remember. Ideally, you want your password to be as many characters as possible and entirely random. Not only that, but experts caution against using the same password for multiple accounts, so the highest level of password security would require a unique, long, random password for every single website you use. Finally, best practices would suggest that you should change your password often to keep identity thieves away.

Remembering so many complex passwords is a nearly impossible task, but not using unique, complex passwords increases the possibility that your personal information could be stolen. If your passwords are too simple or short, it becomes easier for hackers to determine what they are and gain access to whatever information those passwords were protecting. Worse, if you use the same password across multiple accounts and the information is stolen in one place, it could be used to gain access to your other accounts.

A password manager significantly increases your online security, of course, but it also just makes your online life simpler: remembering numerous complicated passwords is challenging for everyone, but a password manager only requires that you remember a single password.

What is a password manager and how does it work?

Password managers create, retrieve, and save extremely secure passwords across all of your online accounts. As a user, you would need to remember just one secure password to log into your password manager, and then the manager itself would create passwords and retain that information for the rest of your accounts. It can also generate and save random answers to security questions, making your account information that much safer. Password managers can also protect information like credit card numbers, CVV codes, and other private details that you may want to have easily saved but encrypted on your computer.

Depending on the password manager and your preferences, your password "vault," or aggregated list of passwords managed by the program, will either be stored securely on the company's servers or locally on your own computer. These managers work on web browsers and on the browser and apps for most mobile devices, so you can use the manager across your devices.

Password managers also allow you to share select passwords with family members or other trusted individuals if you need others to have access to certain accounts. Some managers offer family subscriptions, which allow multiple members to access all or portions of a single shared vault, and others simply allow the user to share individual passwords with selected other individuals.

Are password managers difficult to use?

Setting up a password manager is simple. Once you have chosen your preferred manager, you simply download the program, log in with your email and one long, secure password, and start directing it to your other online accounts. Password managers can typically import any passwords that you may have saved into your browser, and beyond those passwords, you can either save log in information the next time you access a website with a password or enter your account information manually. If you have a large number of online accounts, this process can take some time, so experts recommend starting with your most important accounts right away (like your bank, email, and social media log ins) and working your way through the rest of your accounts as is convenient.

Once the password manager knows about all of your accounts, your work is essentially complete. You can change passwords through the manager as needed, and most managers will also monitor your accounts for attempted security breaches. Some password managers have an autofill feature to make logging into your accounts even easier, though security experts caution that you should not allow autofill except on the most secure websites.

One potential pitfall of password managers is that your one, master password is often not recoverable, so if you forget the password you have chosen, you will be locked out of your vault. You would still be able to access your accounts by changing the passwords for each one of your online accounts, but you would have to set up your password manager all over again if you wanted to continue using it. Once you have chosen your master password, experts recommend that you write it down and store it somewhere secure as a backup.

I want to use a password manager. Which one is best?

Choosing a password manager comes down to your personal preference: experts say that any of the mainstream password managers would provide you with similar security. Below are a few of the more popular password managers.

LastPass
Cost: Free, or $24 per year at the Premium level and $48 per year for families

LastPass is one of the most popular password managers, and it is extremely simple to use. Getting started with LastPass simply involves adding an extension to your browser, choosing a master password, and adding websites you use regularly. With LastPass, you can manage your passwords from any device. The LastPass vault stores all of your login information, as well as digital records you might want to upload like insurance cards, Wi-Fi passwords, and other private data. At the premium level, you receive encrypted storage space, priority customer support, and additional login options.

1Password
Cost: $36 per year for individuals or $60 per year for families

Much like LastPass, 1Password allows you to manage all your accounts and apps as well as save important information like bank account routing numbers in one place. Your passwords sync across all of your devices as well. 1Password is known for having an extremely easy-to-use interface, allowing users to customize their passwords, and warning users of data breaches around the web through its "watchtower" feature. It is more expensive than LastPass, but it provides the kinds of features you would only receive at LastPass's premium level. Interested users can try it free for 30 days.

Dashlane
Cost: Free, or $60 per year for the Premium level

Dashlane is known for having a particularly simple interface to manage your passwords via browser extension or application. Dashlane will also allow you to designate emergency contacts who can access your information, provide alerts when websites report security breaches, and allow some password sharing. Dashlane differs from LastPass and 1Password in that you can easily store your passwords locally instead of on its own servers. If you want to sync your passwords across multiple devices, you would have to upgrade to the Premium level of service.

Conclusion

Protecting your personal information online is essential but challenging, especially in an environment in which individuals and firms regularly suffer hacks and data breaches at an accelerating pace. While you simply cannot protect against every kind of information theft, implementing the use of a password manager is a simple change that can have a significant impact on the safety of your personal information.