Everything You Need to Know About Password Managers

Confused about password managers? They're simpler than you might think.

By Andrew Chaikivsky
February 07, 2017

If you haven't gotten around to using a password manager yet—one of the top safety practices recommended by security experts—you're not alone. Even Lorrie Cranor, the just-departed chief technologist at the Federal Trade Commission, who helped protect consumers from online crimes, only started using one in late 2016. "I've been advocating password managers for years but I'd never actually tried one," Cranor says.

These services can help defend against criminals by generating and storing a different password—one that's long and complicated—for each of your online accounts. But deciding which password manager to trust with the keys to your online life may seem daunting.

The nuts and bolts are confusing, too. Consumers may wonder how to set up the service, where their passwords will be stored, how to share passwords with a spouse, how password managers work with smartphone apps, and more. (I had those questions myself.) Here's a detailed explanation of what you need to know.

What Are Password Managers, Exactly?

The vast majority of us either use weak passwords or reuse passwords on multiple accounts. This makes us more susceptible to crimes such as identity theft. A password manager will generate, retrieve, and keep track of super-long, crazy-random passwords across countless accounts for you, while also protecting all your vital online info—not only passwords but PINs, credit-card numbers and their three-digit CVV codes, answers to security questions, and more—with encryption so strong that it might take a hacker between decades and forever to crack.

And to get all that security, you'll only need to remember a single password, the one you use to unlock your so-called vault. Your login data will be locked down and, at the same time, remain right at your fingertips.

You'll still want to take other security measures, such as setting lock screens on all your devices, using two-factor authentication on valued accounts, and only using computers that you trust.

"Password managers are not a magic pill," Lujo Bauer, a security researcher and associate professor at Carnegie Mellon University, says, "but for most users they'll offer a much better combination of security and convenience than they have without them. Everyone should be using one."

Convinced, but don't know which one to choose? Security experts say you shouldn't overthink it. "As long as it's a name brand"—like 1Password, Dashlane, KeePass or LastPass, the four most popular options— "what password manager you use largely comes down to your personal preferences," says Dan Guido, CEO of digital security firm Trail of Bits. "At the end of

the day, the most important thing is that you find it easy to use so you'll stick to it."

If you try one password manager and don't like it, it's not a huge deal. Each of the big four password managers allows you to export all your data, so if you're not feeling it, you can delete your account and go elsewhere.

What Will One Cost?

You have to pay for some password managers, but not all. Dashlane charges $40 per year to sync one account across all your devices—your home computer, laptop, mobile phone, and tablet. (You can use Dashlane for free, but you won't be able to sync changes after the first month.) 1Password will run you $2.99 a month across all your devices after a 30-day trial period.

Like other password managers, both of these offer strong security: AES-256 encryption, which is used by the federal government to protect classified information. But what you're really paying Dashlane and 1Password for is easy-to-use software with nifty features such as alerts when one of your sites or services has been breached, priority customer service, the ability to change your old passwords automatically on certain sites, seamless syncing, and a smart, engaging interface.

Other services are free. The cloud-based password manager LastPass recently waived its $1 monthly fee; it offers many of the same features as Dashlane and 1Password and will sync your vault across all of your devices. (You'll still have to pony up $12 a year for features such as priority tech support, one

gigabyte of encrypted file storage, and up to five users on an account, which allows for secure password sharing.)

Then there is KeePass (and its Mac-based variant, KeePassX), open-source software that is popular among tech enthusiasts. This option is completely free. It looks like something out of 1995, but that doesn't mean it skimps on security. It protects your password vault with the same strong encryption used by fee-based password managers.

But there's a caveat. KeePass is a DIY password manager—only choose it if you're willing to fiddle. You can find detailed instructions online to walk you through the basic setup, as well as more advanced features that require a mix of tech know-how and patience. But you can't call customer support if you run into problems.

How Do I Set It All Up?

Except for KeePass, getting started with any password manager is roughly the same—and it's simple. With Dashlane and 1Password, you'll first download and install software and an extension for your browser. LastPass requires only a browser extension. You can also download an app for your mobile phone or tablet. It will all take just a few minutes.

To set up an account, you'll use your email address and will need to come up with a master password—a long, random, complicated one.

Next, you'll have to let the password manager know about your various accounts. You'll be able to either import passwords you've stored in your browsers or have the

manager store your username and password the next time you log in to a site, or enter the information manually.

Can a Password Manager Change My Old Passwords for Me?

Changing the old, weak passwords on your many online accounts to burly new, computer-generated ones can be a chore. Both Dashlane and LastPass have a feature that will automatically do this for selected lists of sites, but they are haphazard collections.

To change the majority of your passwords, you'll have to do it yourself: Log on to the site, go to your account information, and let your password manager generate a new long, unique password. While you're at it, it's wise to change the answers to your security questions to nonsense strings of characters (which you can store in your password vault, too).

Replacing all your weak or reused passwords will take time, especially if you're dealing with dozens of accounts. But you don't have to do it all at once. Security experts recommend addressing your most high-value accounts first and then getting around to the other ones when you can. "Even if you've changed your password to only a few sites—like your email, your bank, cloud storage—you've significantly increased your security," Bauer says.

As you add accounts to your vault, you'll see that password managers also store the URLs for sign-ins, a very useful security feature: Many phishing attacks try to trick users into submitting account information by directing them to

fraudulent websites with slightly different web addresses. Instead of clicking on links in a suspicious email, use the link stored in your password manager to sign in, or type the URL yourself.

Another nifty and potentially time-saving feature: A password manager's browser extension can automatically fill in your user info. It can even automatically log you in to your account, though security experts warn that users should tread carefully here. It's usually safer to disable auto-logins through the manager's settings.

"Web browsers are huge pieces of software with complex functionality," Bauer says. "With automatic logging-in, you're effectively forced to trust web browsers not to trick the password manager into divulging your password. It is much safer to have a prompt so that you have to actively agree before your password manager sends a password to a website."

Where Will My Passwords Be Stored?

This is a big dividing line between approaches with password managers. It's a matter of local vs. cloud-based storage—you can either keep all your passwords on a laptop or a storage drive at home, or remotely on a company's servers.

By default, LastPass, 1Password, and Dashlane store your password vault on their servers, allowing you to easily sync your data across devices. As a second benefit, if your computer crashes you won't lose your vault.

But some people just really hate the idea of storing all their passwords on one site in the cloud—no matter what the company promises about its security measures, there's probably a bulls-eye painted on its encrypted back. If that sounds like you, it's possible to store your passwords locally.

Dashlane lets you do this by disabling the “Sync” feature in Preferences. This will delete your vault and its contents from the company’s servers. Of course, any further changes you make to your vault on your computer won’t show up on your other devices.

Another option: You can purchase a software license from 1Password for a one-time fee of $64.99, which will give you complete control over where you store your vault. To transfer your data to a mobile device, you can upload your encrypted vault manually to a cloud-based storage service of your own choosing, such as Dropbox or iCloud. Then, for peace of mind, you can permanently delete your password vault from the cloud once you’ve moved the data to your phone or tablet.

KeePass is the pure local play. It parks your encrypted vault on your own computer, and you’re free to keep it wherever you choose. There are methods for transferring your KeePass password file so you’ll be able use it on your mobile phone. For instance, the iOS app MiniKeePass can send the vault to your iPhone via iTunes.

How Do I Sign In to Apps?

Password managers work easily in a web browser on your laptop. But you probably want to log in to apps, too, from

Facebook to banking sites. How you do this varies with the kind of phone you use.

Android phones let you use Dashlane or LastPass to log in to your apps automatically, after making a few simple tweaks to your settings; 1Password can fill in your usernames and passwords with a tap of a key on a dedicated keyboard.

Apps on iPhones are a different story. Although a few hundred are supported for autofill with 1Password, Dashlane, and LastPass, chances are that many of the apps you use are not supported.

But this doesn't mean you're locked out of those apps. At worst, you'll have to toggle between your password manager's app and, say, your banking app, copying and pasting your username and password. It sounds onerous, but after only a few taps you're logged in, and you'll never have to type in a long, complicated password again.

Can My Spouse and I Share Passwords?

While it's good security practice always to keep your passwords to yourself, there are times when you'll need to share one with a family member or coworker. Some password managers are better than others at doing this securely.

KeePass, for example, isn't designed for discrete password sharing with a non-KeePass user. You can store a database of shared passwords in the cloud, but this means you might have to set someone up with KeePass.

1Password has a Families subscription option for up to five members at $4.99 per month (if you start with an individual plan you can migrate it to a Families plan later). You invite family members via email and can provide them with customized levels of access—like banking sites for the grown-ups only, gaming services for the kids, and streaming services for everyone. Family members will have to download 1Password onto their devices and establish their own master passwords, and your family's vault will be stored on the company's servers, with any changes synced immediately across everyone's devices.

Both LastPass and Dashlane let you share as many individual passwords as you want with nonusers (although they'll have to sign up for a free account to retrieve the login info) and your sensitive data will be encrypted throughout its journey. However, the nonpremium, free versions place limits on users—if you're not paying for premium Dashlane features, for example, you can only share five items with someone.

What If I Forget My Master Password?

Only LastPass will offer you a password hint (or a way to reset the master password, if you're on a device you've used previously).

But for the other managers, forgetting your master password means you're locked out of your vault forever. Which is bad news, but not the end of your online world—lock yourself out of your vault and you'll just have to reset all of your passwords, account by account, site by site.

To be safe, write your master password down and store it away in a secure place.

C'mon, Can't You Just Tell Me Which Password Manager to Use?

It really does come down to personal preference. While interviewing a half-dozen security experts, I found that one swore by 1Password, two were devoted KeePass users, one told me to "just use LastPass," and one used Dashlane. There was no consensus.

So I decided to try out all four of them myself. Setting up 1Password, Dashlane, and LastPass and their browser extensions really was easy and quick. (I put off dealing with KeePassX because of all I'd read about it being for tech experts only.) But while the ease-of-use features like auto-fill and generating passwords were helpful, at times it seemed too frictionless, as if an invisible hand were reaching down into web pages, filling in boxes and logging into my accounts on its own. It was unsettling.

Then there was the price. Sure, these services only cost a few dollars a month, and that's less costly than getting clobbered by an identity theft. But over a few years it would add up to $400 or more. And who wants to spend money on *passwords?*

Finally, I sat down to try to figure out Keepass. Five minutes in and I was ready to give up. Was I downloading the right version? Could this actually be malware? But after awhile I found a very helpful guide through Security in a Box, a project founded by two human-rights groups. It offered step-

by-step instructions that made setting up Keepass about as challenging as putting together an Ikea bookcase.

To integrate Keepass with a web browser I would have needed a separate plug-in, but I already had all the features that I really wanted–strong encryption, a password generator, and one place to store account info, PINs, and security questions. Good enough for me. What's more, I didn't have to trust someone else's servers. While I have no doubt that commercial password managers are taking the most stringent security measures, I just feel much more comfortable keeping access to my vault completely in my own hands.

And there were other benefits. Once I got KeePass up and running, I not only had a great password manager, I also felt a hard-earned sense of tech-insider satisfaction. It didn't cost me a dime.
