Unknown date | **Unknown author**

These are the best password managers.

Because reusing passwords is dangerous.

Do you hate creating and remembering your passwords? Here's the solution.

cc

The Post's Geoffrey A. Fowler shows you how password managers are a much better (and more secure) way to manage your passwords to your favorite sites. (Jhaan Elker, Geoffrey Fowler/The Washington Post)

Pardon the interruption, but your passwords are leaking.

You've probably become numb to all the headlines about data breaches. But a website called Have I Been Pwned will expose the horror they've wreaked on you.

Type in your email address and Have I Been Pwned lists websites and apps on which your passwords have been compromised. ("Pwned," pronounced like "owned," is geek speak for conquered.) Try your family members' emails and your favorite passwords, too. Australian security guru Troy Hunt spends his days looking in dark corners of the Internet to add hacked data to this free site. It now totals half a billion exposed passwords and 5 billion hacked accounts. Hunt can hardly keep up.

Aside from freaking out, what are you supposed to do?

We've gotten a lot of hard-to-follow password advice over the years. Change them every 90 days. Make them really long. Add in rAnDoM #@s! Hunt's site proves one rule is more important than all the others in a world where breaches are unavoidable: **Never, ever reuse a password.**

It makes sense, if you think like a hacker. When they get their grubby paws on a password from one site, they go and try it on other sites. If you've used that password somewhere else, the bad guys may also have access to your email, your bank account — your life.

Sure, but we now use dozens of websites, maybe hundreds. My brain can't hold that many passwords — I can't even keep track of all the dead characters on "Game of Thrones." People try all kinds of unwieldy tricks to stay on top of passwords: Post-its or a notebook are easy to lose, hard to update, and often not around when you need them. Saving passwords in email, Word documents or spreadsheets is not very secure. One of my colleagues (she knows who she is) clicks the "forgot your password" button every time she needs to log in.

There is a better way. Most security gurus I know use a password manager. It's a program that keeps all your passwords in one digital safe-deposit box. Aside from being the memory you wish you had, a password manager will save you time by typing in passwords for you across many devices. And fresh updates are making these programs simpler and more useful than ever.

When you use the Dashlane password manager, a plug-in for your Web browser looks for spots to log in and fills them in for you, saving you a few seconds of typing and clicking. (Dashlane)

This isn't as hard as you think

Perhaps getting a password manager is already on your radar. Maybe it sounds a little risky. Maybe it sounds like too much work. I took the plunge, and it was definitely less work than cleaning out the garage, and less expensive than the Frappuccino I rewarded myself with afterward.

First, you have to stop clicking yes when your Web browser asks "Would you like us to remember your password?" Enticing as it sounds, that doesn't help your passwords stay up to date everywhere — on your office PC or your iPhone. Apple and Google have their own password managers that pop up in Safari and Chrome, called iCloud Keychain and Google Smart Lock, but they work only if you live in all-Apple or all-Google worlds.

After testing password managers that work across browsers and devices, I recommend one called Dashlane. It's the one simple enough that you're likely to stick with it, though its features are neck and neck with rivals 1Password and LastPass, which are also fine choices.

Dashlane, used by 10 million people, is free to try on a single device. You pay a subscription to make it securely sync up your passwords (and other secrets such as credit card details and ID numbers) across your computer, phone and tablet. At $3.33 per month, Dashlane happens to be the most expensive of the three, but like the Apple of the password game, its design and customer service are worth it.

Dashlane also has been largely free of drama over its own security. You would be right to wonder how safe it is to keep all your password eggs in

one basket. All three of these companies keep your passwords encrypted behind a password they don't know — so that even if they get hacked, the data is mostly useless. They never send your password over the Internet. In 2015, LastPass reported it was breached, though it reported that no passwords were stolen. There are no security guarantees, but I buy the argument that it's okay to keep your eggs in one basket if it's more secure than the basket you build on your own.

The biggest hurdle is changing your habits. With a password manager, you don't memorize passwords — you retrieve them from an app. Let that sink in: You won't remember your Gmail password anymore, but you'll be better off because now your password can be a long bunch of gobbledygook that's harder to crack.

Here's how it works

I recommend getting started on a Mac or Windows PC, where it's easier to see what's going on. The process of setting up Dashlane is pretty similar to 1Password and LastPass, despite some other design differences.

After you download and install the Dashlane app comes the most important step: You have to choose a "master password," a key that unlocks the digital safe holding your passwords. Make it a good one — and whatever you do, don't forget it. Since the password manager company doesn't know your master password, it can't reset it.

Whenever you open Dashlane, or use it to fill in sensitive information such as credit card numbers, it will ask you for your master password. On devices with fingerprint readers and face identification, you can bypass typing it in by scanning yourself instead.

Next, Dashlane will guide you to install a plug-in for your Web browser. There, it ingests any old passwords you've saved in the browser and then hangs out, watching for you to type in log-ins and passwords and learning them, or offering to help generate a unique, secure password. (You can see Dashlane working when it puts its logo — a dashing impala — in a text-entry field.) You can teach it a whole bunch of passwords right away, or just hang back and let Dashlane learn them over time.

Now the magic happens. The next time you go to a site where Dashlane has memorized your password, it will automatically fill it in for you. This is a time saver and works about 95 percent of the time. When it doesn't work, you have to open the Dashlane app to copy and paste your password into the website. It's an annoyance but not a dealbreaker.

Dashlane can't fill in the password to log in to your computer, or type in the PIN on your phone. If you decide you don't like it, you can export your password list to move it to another program — or even print out your list and live off that.

Dashlane scours your trove of passwords for ones that could use improvement and assigns you a security score. (Dashlane)

They're getting easier and more helpful

People who've tried and given up on password managers often complain about the difficulty using them on their phones. But in recent months, they've made some big inroads for simplicity.

With Apple's iOS 12, you can now use a password manager such as 1Password to automatically remember and enter your log-ins and passwords in the browser and in apps. (1Password)

It used to be that every time you needed to log in to an app on your phone, you had to launch the password manager to manually copy and paste your username and password. But last year, Android O added the ability for third-party password managers to automatically fill in those details. Last month, Apple announced its iOS 12 will offer a similar capability, and Dashlane, LastPass and 1Password all showed me how it will work when it becomes widely available this fall. When you need to log in through an app or website, an auto-fill option from your chosen password manager will pop up right above the keyboard. You tap and go.

Password managers can also make your life easier in a few other ways. All three of the ones I recommend can share passwords with other family members and co-workers who use the same program. Dashlane and LastPass also let you identify emergency contacts — people who, after a period of time you determine, will be able to access your passwords and

other saved information. This can make accessing bank, email, social media and other personal information much less stressful after a death.

Beyond just remembering passwords, these programs are also getting deeper into the business of keeping you safe. They'll analyze your trove of passwords, give you a grade on their security and politely prompt you to change passwords when they are reused or weak, or when sites report they've been hacked. 1Password recently began working with Have I Been Pwned to flag and stop you from using passwords that are known to have been compromised.

If getting a password manager inspires you to do even more about online security, there are further steps you can take. I also recommend turning on what's called "two-factor authentication" everywhere it's available — it will ask for an extra code when you log in and flag whether someone else is trying to get into your account. But if that's not available on sites you use frequently, you should pat yourself on the back for at least getting your passwords shipshape. Now about cleaning out the garage …

Price: Free to use on one device; $3.33 per month, billed annually, to sync your data across multiple devices.
Likes: Simple, slick design. Offers live chat support Mondays through Fridays in addition to email support every day. Saves receipts for online purchases.
Dislikes: Most expensive option, and no discounted family plan.

Price: Free trial for 30 days; $3/month.
Likes: Strong reputation for security. Comes with pro-level controls, including the ability to sync passwords across devices without the cloud.
Dislikes: It's more complicated. Security measures prevent auto-filling and auto-submitting passwords without an additional click. Cannot auto-change passwords.

LastPass •••|

Price: Free to use, including syncing; $2/month adds features including sharing passwords.

Likes: The best free option, covers most of what you need. Can store encrypted files in notes, such as PDFs.
Dislikes: Has encountered the most high-profile breaches and bugs, though it responded to them quickly.

Read more tech reviews and analysis from Geoffrey A. Fowler:

Hands off my data! 15 default privacy settings you should change right now.

Meet the future phones that fold up, have 9 cameras and charge over thin air.

Why you cannot quit Amazon Prime — even if maybe you should
