The New York Times

WIRECUTTER

Why You Need a Password Manager. Yes, You.

Everyone should use a password manager. It's the most important thing you can do — alongside two-factor authentication — to keep your data safe.

By Andrew Cunningham
Mr. Cunningham is a lead editor at Wirecutter, the product recommendation site owned by The New York Times Company.

Published Aug. 27, 2019 Updated Sept. 2, 2019

You probably know that it's not a good idea to use "password" as a password, or your pet's name, or your birthday. But the worst thing you can do with your passwords — and something that more than 50 percent of people are doing, according to a recent Virginia Tech study — is to reuse the same ones across multiple sites. If even one of those accounts is compromised in a data breach, it doesn't matter how strong your password is — hackers can easily use it to get into your other accounts.

But even though I should know better, up until a few months ago I was still reusing the same dozen or so passwords across all of my everything (though at least I had turned on two-factor authentication where I could). It's just too difficult to come up with (and remember) unique, strong passwords for dozens of sites. That's why, after much cajoling from co-workers, I started using a password manager — and it's why you should be using one, too. Aside from using two-factor authentication and keeping your operating system and Web browser up-to-date, it's the most important thing you can do to protect yourself online.

Why you need a password manager

A password manager is a secure, automated, all-digital replacement for the little notepad that you might have all of your passwords scribbled down in now, but it's also more than that. Password managers generate strong new passwords when you create accounts or change a password, and they store all of your passwords — and, in many cases, your credit card numbers, addresses, bank accounts, and other information — in one place, protecting them with a single strong master password. If you remember your master password, your password manager will remember everything else, filling in your username and password for you whenever you log in to a site or app on your phone or computer.

You can generate, save, and auto-fill passwords with Google's Smart Lock (in Chrome and Android) or Apple's Keychain (in Safari and iOS), but a good password manager goes a lot further — it can proactively alert you when you're reusing a password or when your passwords are weak and easy to guess or hack, and some password managers will even let you know when online accounts are hacked and your passwords have been exposed. For accounts that you need to share with family members, friends, or co-workers — a joint bank account or mortgage site, a shared Twitter account, or your insurance and medical records, for instance — many password managers offer family plans that make it simple to share strong, complex passwords without requiring multiple people to remember them or write them down.

Learning to use a password manager seems intimidating, but once you start using one to make strong random passwords that you're not on the hook to remember, you'll wonder how you lived without one. Usually, improving your digital security means making your devices more annoying to use; a password manager is a rare opportunity to make yourself more secure and less annoyed.

A password manager for any budget

Wirecutter's favorite password manager is 1Password. It has great apps for PCs, Macs, and all kinds of tablets and phones, and those apps will tell you exactly what's wrong with your passwords and how to fix them, whether they're weak, reused, or even compromised in a hack. If you're not using two-factor authentication to further protect your accounts already, 1Password can generate, store, and insert those codes for you when you need them. And 1Password's family plan makes it easy to share passwords for accounts you share with your family members and friends (and to keep their passwords safe, too).

If you can't or don't want to pay the $36 per year for a 1Password subscription, you can find good free options too. Wirecutter's favorite is LastPass Free — its apps aren't as full-featured as 1Password's, and its recommendations for fixing password problems aren't as clearly explained or as easy to act on, but it's still pretty simple to use and it still works on just about any computer, tablet, or phone.

These aren't the only good password managers out there, but these two are easy to learn, backed by good customer support, and designed to store your passwords securely. You don't need to understand hashing or AES-256 encryption, except to know that it means that even if 1Password or LastPass has its servers hacked, your passwords will remain unreadable to anyone who doesn't have your master password. Both 1Password and LastPass are transparent about their security processes, and you can visit their sites to learn more.

Making a good master password

Because your master password is responsible for protecting all of your account information, you must make it long and difficult to guess. But because you'll need to type it in when you start using a new computer or phone, when you need to log in to change account settings, or when you restart your computer or browser, it should also be easy for you to remember; otherwise you could lock yourself out of your account and lose access to everything.

Both 1Password and LastPass have good advice on how to make a master password, and perhaps surprisingly, they don't recommend long strings of random lowercase and uppercase letters, numbers, and symbols. Instead, you need a long but memorable password, perhaps composed of multiple random words with dashes, periods, or some other easy-to-remember punctuation in between, like "discard-memento-burble-pacer." 1Password's password generator is a handy way to make one of these passwords regardless of the software you use.

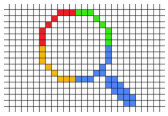
No matter how memorable your master password is, you should write it down and store it somewhere to make sure you don't forget or lose it. The most secure way to do this is to write it on an actual piece of paper and keep it somewhere safe, such as a locked desk drawer or Wirecutter's recommended fireproof document safe. Writing it down the old-fashioned way is actually much more secure than storing it digitally, especially on a cloud syncing service such as Google Drive, Dropbox, or iCloud; 1Password even has a handy "emergency kit" printout that tells you exactly what you need to write down.

Sign up for the Wirecutter Weekly Newsletter and get our latest recommendations every Sunday.

A version of this article appears at Wirecutter.com.

Protecting Your Internet Accounts Keeps Getting Easier. Here's How to Do It. March 27, 2019

6 Google Tricks That Will Turn You Into an Internet Detective Aug. 21, 2019



A School Laptop Under $500 That Isn't Junk Aug. 6, 2019

A version of this article appears in print on Sept. 2, 2019, Section B, Page 5 of the New York edition with the headline: Everyone Needs a Password Manager