Password managers: A little pain for a lot of security

They're your friend, or at least a helpful acquaintance.

Laura Hautala

March 10, 2020 5:00 AM PDT

- 2

Don't use bad passwords, use a password manager.
Stephen Shankland/CNET

If you're one of the countless people who unwisely use easy-to-guess passwords or reuse a password for several accounts, cybersecurity

experts have a message for you: It isn't your fault. Memorizing a unique, complex password for each account is impossible.

But that's exactly the sort of chore computers are good at. That's why many cybersecurity experts suggest using a password manager. It's a software utility that securely stores passwords and automatically fills them into login pages. They help you protect every single one of your online accounts with a strong password.

"I recommend everyone use it," said Matias Woloski, chief technology officer of authentication firm Auth0 and an expert in password security. "Password managers are today the best alternative."

You'd probably benefit from password manager help. The most-used password found in data breaches is still "123456", according to data from cybersecurity firm SplashData, and the second most common password is, of course, "password". The average person uses only 13 unique passwords, and almost a third said they only use two or three passwords for all their accounts, according to a 2018 survey from antivirus software company McAfee.

For a broader look at the situation, check this week's CNET coverage of today's password problems, including improvements like security keys and the shortcomings of two-factor authentication.

You've got several password manager options. There are dedicated tools like LastPass, BitWarden, Dashlane, Keeper and 1Password. Web browsers including Safari, Chrome and Firefox also have built-in password controls that are more limited, especially if you use multiple browsers, but they're getting more sophisticated.

Unfortunately, password managers can be complex and don't always work smoothly with websites and apps. That might be why only 3% of internet users rely primarily on password managers, according to the Pew Research Institute. Woloski suggests you get started with help from someone more technical.

Still, password managers can help you navigate the internet with a lot less risk. Even though the tech industry is finally coming up with real alternatives to passwords, and ways to dump them altogether, you'll still have to reckon with dozens of them, or hundreds, for years to come. Password managers can help, even if they aren't perfect

What's a password manager?

Password managers generate unique, complex passwords for every site, store them securely and enter them on different browsers and computing devices. You can use them as browser extensions or mobile apps that fill out login pages with your username and password for you.

READ MORE

- **The best password managers for 2020 and how to use them**

There are tons of benefits. First, you don't have to memorize any passwords (except for the password to your password manager). That

means you can actually follow unpleasant but useful security advice, like never reusing a password and always using long, complex passwords like $ZnEk$tyMcF6K6XCGkxU3A8>uzC[B6&X.

Next, password managers help guard against phishing attacks that direct you to fraudulent websites and try to trick you into entering your password. Password managers offer your login credentials only when you're at the correct website.

Finally, many password managers have features that tell you when a site has experienced a data breach. They can also tell you if the password you're using has been found in a stockpile of stolen user data, as at least 555 million passwords have. Those are signs you need to change your password immediately. Password managers also can help you find weak or reused passwords.

Should you store all your passwords in one place?

The standard advice for decades has been to memorize passwords, so storing them in one place feels a little wrong. And, of course, it would be terrible if hackers could breach your password manager and access all of your accounts.

Still, the security of password managers has proven to be robust. Hackers have only made limited headway in stealing user information from password managers -- one breach got as far as compromising the hints for LastPass' user security questions, for example -- but no known attacks accessed caches of actual passwords.

Sure, hackers could eventually break that security, but they're much more likely to target you with a phishing attack to steal your passwords, said Mark Risher, Google's head of account security. Plus, using a password manager limits the chances you'll fall for a phishing attack.

Now playing: In a world of bad passwords, a security key could be...
4:11

Of course, you need to be careful. With all your password eggs in one password manager basket, make sure you find a way to remember your master password or secret key. It's OK to write it down as long as you keep it somewhere safe. You can also export your passwords to a spreadsheet from time to time, as long as you lock it away with encryption (or put a printed copy in a locked file drawer).

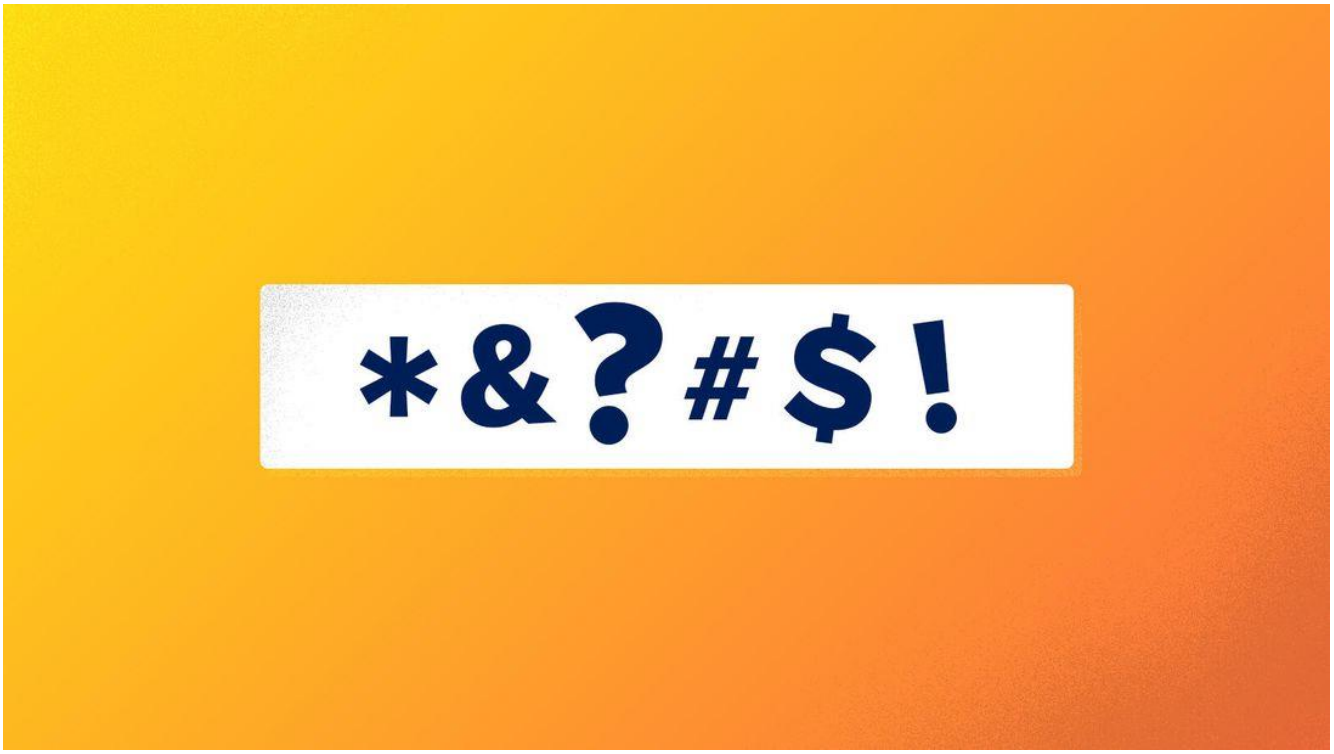
If you do lose access to your account, you'll have to go through the password reset process for all your other accounts, which would be a very big headache.

Password manager drawbacks

Unfortunately, you should expect rough patches when using password managers. Just adding information from all of your existing accounts to the service is work, though most password managers offer tools to import the data from your browser or other password managers. And it takes extra steps to enable your password manager on your phone.

Perhaps the biggest issue is that some websites don't play nice with password managers, causing the kinds of fiddly, obnoxious problems that make you want to throw your computer out the window.

For example, password managers sometimes don't notice login fields. Or they can fumble when websites ask for extra information like a PIN code or your favorite movie.



Sometimes web pages don't play nice with password managers.
Brett Pearce/CNET

Worse, some websites block the autofill feature, keeping password managers from entering your login credentials. One Australian bank, CommBank, advises customers not to store their bank account credentials on a password manager. In a statement, CommBank said it sees the value of password managers, but believes hackers will find ways to trick its customers with sophisticated phishing schemes if they use password managers.

"For online banking passwords, we recommend customers create a strong password that is unique to each account and do not write this down," a company spokesperson said. Still, security experts say this makes it much more likely that customers will use weak or reused passwords.

1Password is tackling autofill blocking by working with web browser makers that want to make websites allow the feature, said Matt Davey, the company's chief operations officer.

"What they're trying to do is override them on a site level, and autofill them anyway," Davey said of browser makers. 1Password will also contact websites directly and tell them they should get with the program and let their users log in with a password manager.

Even technically skilled people struggle with the friction of password managers. Kimber Dowsett, a cybersecurity expert who previously helped secure NASA systems and now works as a consultant, got frustrated recently when she tried to log into a bank website. She had to type in her login credentials manually, because the website blocked her password manager.

There was one final problem: She couldn't tell if a character password was the number zero or the letter O, so she had to guess.

"A lot of the friction would be alleviated by app developers just allowing autofill and paste so that we could actually use password managers as intended," Dowsett said. "Throwing a wrench into it isn't helping any of us."

Using passwords less

There's good news on two fronts. The first is that the makers of Chrome, Safari and Firefox are beefing up their own password managers. Apple has built one into iOS and enables it by default. It's OK to use these features on devices that you control with a password or biometric login. Plus, they should make digitally storing passwords more mainstream and potentially force website developers to play nice with features like autofill and paste.

Second, new technologies let you use passwords less. Biometrics like your fingerprints and face reduce the need to present your password every time you access a service. Single sign-on services let you log onto one site with another account, like Google, Apple or Facebook. You'll have to be comfortable sharing more information about the services you use with one of these tech titans, though.

Third, multifactor authentication, security keys and other authentication technologies are helping improve the security shortcomings of passwords. Eventually, you might not have to use passwords at all.

This innovation isn't replacing passwords anytime soon, said BigID CEO Dimitri Sirota, whose company helps businesses protect personal information. But it's starting to chip away at the primacy of passwords for keeping your accounts safe. And that's a good thing, he said.

"Passwords have been the standard for a long time," Sirota said. "And one that no one's particularly happy about."