cnet.com

Keep Your Passwords Strong and Secure With These 9 Rules

Clifford Colby Managing Editor

8–10 minutes

A strong password is essential when it comes to your online security, and you need a unique one for each of your social media, bank accounts, streaming services and apps. But with so many accounts to keep track of, it's tempting (and incredibly easy) to fall into the bad habit of using the same login credentials for everything.

If your data is compromised, weak passwords can have serious consequences like identity theft. Last year's number of reported data breaches set a new record -- not to mention the T-Mobile hack in 2021 that exposed more than 50 million customers'

personal information.

The identity protection of a post-password world isn't here for most of us. So in the meantime, try these best practices that can help minimize the risk of your data being exposed. Read on to learn how to create and manage the best passwords, how to be alerted if they're breached, and one crucial tip to make your logins even more secure. And here are three old password rules that wound up being dumb today.

Read more: Best Password Managers for 2022 and How to Use Them

Use a password manager to keep track of your passwords

Strong passwords are longer than eight characters, are hard to guess and contain a variety of characters, numbers and special symbols. The best ones can be difficult to remember, especially if you're using a distinct login for every site (which is recommended). This is where password managers come in.

A trusted password manager such as 1Password or Bitwarden can create and store strong, lengthy passwords for you. They work across your desktop and phone.

ht-broida-passwords

A good password manager can help you keep track of your login info.

The tiny caveat is that you'll still have to memorize a single master password that unlocks all your other passwords. So make that one as strong as it can be (and see below for more specific tips on that).

Browsers like Google's Chrome also come with password managers, but our sister site TechRepublic has concerns about how browsers

secure the passwords they store and recommends using a dedicated app instead.

Password managers with their single master passwords are, of course, obvious targets for hackers. And password managers aren't perfect. LastPass fixed a flaw in 2019 that could have exposed a customer's credentials. To its credit, the company was transparent about the potential exploit and the steps it would take in the event of a hack.

Read more: Why Password Managers Are Great Until You Lose Your Password

Yes, you can write your login credentials down. Really

We know: This recommendation goes against everything we've been told about protecting ourselves online. But password managers aren't for everyone, and some leading security experts, like the Electronic Frontier Foundation, suggest that keeping your login information on a physical sheet of paper or in a notebook is a viable way to track

your credentials.

And we're talking about real, old-fashioned paper, not an electronic document like a Word file or a Google spreadsheet, because if someone gains access to your computer or online accounts, they can also gain access to that electronic password file.

cybersecurity-hacking-16

Keeping passwords on a sheet of paper or in a notebook might work best for some people.

Graphic by Pixabay/Illustration by CNET

Of course, someone could also break into your house and walk off with the passkeys to your entire

life, but that seems less likely. At work or at home, we recommend keeping this sheet of paper in a safe place -- like a locked desk drawer or cabinet -- and out of eyesight. Limit the number of people who know where your passwords are, especially to your financial sites.

If you travel often, physically carrying your passwords with you introduces greater risk if you misplace your notebook.

Read more: 5 Ways to Make Your Passwords Instantly More Secure

Find out if your passwords have been stolen

You can't always stop your passwords from leaking out, either through a data breach or a malicious hack. But you can check at any time for hints that your accounts might be compromised.

Mozilla's Firefox Monitor and Google's Password Checkup can show you which of your email addresses and passwords have been

compromised in a data breach so you can take action. Have I Been Pwned can also show you if your emails and passwords have been exposed. If you do discover you've been hacked, see our guide for how to protect yourself.

dark-web-image

Watch this: Are your login credentials on the dark web? Find out right now

02:08

Avoid common words and character

combinations in your password

The goal is to create a password that someone else won't know or be able to easily guess. Stay away from common words like "password," phrases like "mypassword" and predictable character sequences like "qwerty" or "thequickbrownfox."

Also avoid using your name, nickname, the name of your pet, your birthday or anniversary, your street name or anything associated with you that someone could find out from social media, or from a heartfelt talk with a stranger on an airplane or at the bar.

Longer passwords are better: 8 characters is a starting point

8 characters are a great place to start when creating a strong password, but longer logins are better. The Electronic Frontier Foundation and security expert Brian Krebs, among many others, advise using a passphrase made up of three or

four random words for added security. A longer passphrase composed of unconnected words can be difficult to remember, however, which is why you should consider using a password manager.

Read more: Strong Passwords Aren't as Easy as Adding 123. Here's What Experts Say Really Helps

Don't recycle your passwords, seriously

It's worth repeating that reusing passwords across different accounts is a terrible idea. If someone uncovers your reused password for one account, they have the key to every other account you use that password for.

The same goes for modifying a root password that changes with the addition of a prefix or suffix. For example, PasswordOne, PasswordTwo (these are both bad for multiple reasons).

By picking a unique password for each account, hackers that crack into one account can't use it to get access to all the rest.

Avoid using passwords known to be stolen

Hackers can effortlessly use previously stolen or otherwise exposed passwords in automated login attempts called credential stuffing to break into an account. If you want to check if a password you're considering using has already been exposed in a hack, go to Have I Been Pwned and enter the password.

No need to periodically reset your password

For years, changing your passwords every 60 or 90 days was a long-accepted practice, because the thinking went that was how long it took to crack a password.

But Microsoft now recommends that unless you suspect your passwords have been exposed, you don't need to periodically change them. The reason? Many of us, by being forced to change our passwords every few months, would fall into bad

habits of creating easy-to-remember passwords or writing them on sticky notes and putting them on our monitors.

Use two-factor authentication… but try to avoid text message codes

If thieves do steal your password, you can still keep them from gaining access to your account with two-factor authentication (also called two-step verification or 2FA), a security safeguard that requires you enter a second piece of information that only you have (usually a one-time code) before the app or service logs you in.

google-authenticator

Google's Authenticator app steps up your security.

Jason Cipriani/CNET

This way, even if a hacker does uncover your passwords, without your trusted device (like your phone) and the verification code that confirms it's really you, they won't be able to access your account.

While it's common and convenient to receive these codes in a text message to your mobile phone or in a call to your landline phone, it's simple enough for a hacker to steal your phone number through SIM swap fraud and then intercept your verification code.

A much safer way to receive verification codes is for you to generate and fetch them yourself using an authentication app like Authy, Google Authenticator or Microsoft Authenticator. And once you're set up, you can choose to register your device or browser so you don't need to keep verifying it each time you sign in.

When it comes to password security, being proactive is your best protection. That includes knowing if your email and passwords are on the dark web. And if you discover your data has been exposed, we guide you through what to do if hackers have gained access to your banking and credit-card accounts.