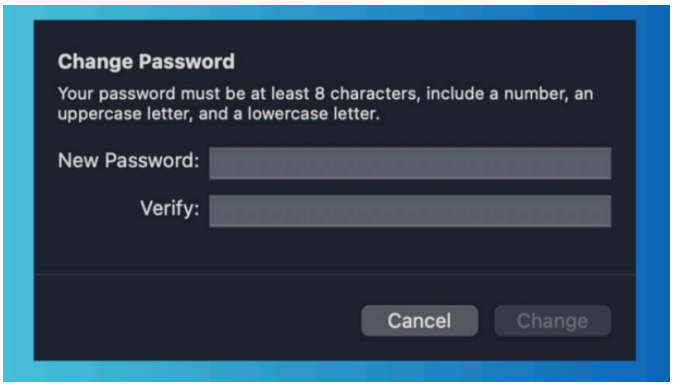
Changing Your Passwords Isn't the Security Measure You Think It Is

You're probably just wasting your own time.

Jake Peterson. February 6, 2025



Credit: Lifehacker

There's a lot of advice out there for proper password management: Each of your passwords should be strong and unique; use a secure manager to store your passwords; use two-factor authentication (2FA) to add an extra layer of security to your accounts. But there's another piece of advice that is held in the same regard as the others: Change your passwords often—perhaps once every three months. This habit is so emphasized, many companies and organizations will make you change your passwords multiple times a year in the name of security. The thing is, in all likelihood, this isn't actually doing anything to help your security.

This idea that changing your passwords multiple times a year is a cornerstone of your security, might be engrained in some of you. After all, it's not new advice. As PCMag examined, the practice goes back a long time: When security experts write about passwords, they often write about changing passwords, too. It's just the way the advice has been presented. But that's likely because it's anticipating and responding to bad security habits.

Good passwords don't (usually) need to be changed

Changing your passwords really only makes sense when your passwords are compromised. After all, if no one knows your password, why change it? Still, passwords are cracked all the time. As such, it might seem logical to frequently switch yours up: You never know which of your passwords could be guessed, right? So might as well keep those bad actors on their toes.

But let's take a step back: There's no reason any of your passwords should be guessable. If a hacker is able to guess your password, **it's a bad password**, and you shouldn't have been using it in the first place. I'll take it a step further, and say none of your passwords should be crackable by a computer, either—at least, not on a timeline where it matters.

A good password, meaning one that is both strong and unique, is inherently uncrackable. It should be long, varied, and not in use on any other account. It shouldn't matter if the companies that control one of your accounts is breached, because this password is different than that one. You can use a tool like Bitwarden's password tester to see how long different passwords take a computer to crack. "Lifehacker" takes eight seconds to crack. "Lifehackerdaughtcalm" takes centuries.

If your password is strong and unique, and takes longer than a human lifetime to theoretically crack, there's no need to change that password in three months time. There's no need to change that password in a year. There's no need to change that password period—unless you're presented with an actual threat.

When to change your password

I'm not saying you should never change your password. You should definitely change it if other people know about it. Most often, that happens when the company that holds your account has a data breach. Let's say AT&T has a mega breach, and authentication data from users is leaked onto the dark web. In that case, you should change your password ASAP. In an event like this, the company in question will probably tell you to do as much, and may even offer you extra perks to make up for the inconvenience of having your data leaked.

Of course, data breaches aren't the only times good passwords are discovered. Malware is another threat to look out for. If you fall for a phishing scam, for example, and download malware to your computer, it may monitor and steal your passwords to your sensitive accounts. Or, you may be tricked into opening a fake version of a website you have an account for, typing your username and password into that site, and presto: password compromised.

In these cases, your strong and unique password has fallen, so yes, it's time to change it. But barring an actual reason to do so, you don't need to bother with switching it up.

To be clear, you're not hurting your security by changing your passwords. In fact, you might not even have a choice, if your company or organization requires you to change your password every so often. But so long as all of your passwords are strong and unique, and none of them are compromised, you're just giving yourself more work without any real gains.

Security tips that won't waste your time

Want some real security gains? Store all those strong and unique passwords in a secure password manager. That way, you only need to remember one strong and unique password—the master key to your password manager. In addition, use two-factor authentication (2FA) whenever possible. 2FA requires a trusted device for secondary authentication after providing the correct password. That way, even if a

bad actor knows your password, they won't be able to break in without access to your trusted device. (Just prioritize an authenticator app or security key over SMS authentication.)

If it's an option for your accounts, you may want to explore passkeys over passwords, too. Passkeys effectively combine the convenience of passwords with the security of 2FA: They generate a key on your trusted device, which is required when signing into a site. That way, there's no password to steal. As long as you authenticate yourself on the device—say, through Face ID or a PIN—you're in.

As long as you make sure each of your accounts is secure using these steps, and you're aware of any data breaches, there's no reason to worry about changing your passwords every three months. Stay secure out there.

Senior Technology Editor

Jake Peterson is Lifehacker's Senior Technology Editor. He has a BFA in Film & TV from NYU, where he specialized in writing. Jake has been helping people with their technology professionally since 2016, beginning as technical specialist at New York's 5th Avenue Apple Store, then as a writer for the website Gadget Hacks. In that time, he wrote and edited thousands of news and how-to articles about iPhones and Androids, including reporting on live demos from product launches from Samsung and Google. In 2021, he moved to Lifehacker and covers everything from the best uses of AI in your daily life to which MacBook to buy. His team covers all things tech, including smartphones, computers, game consoles, and subscriptions. He lives in Connecticut.