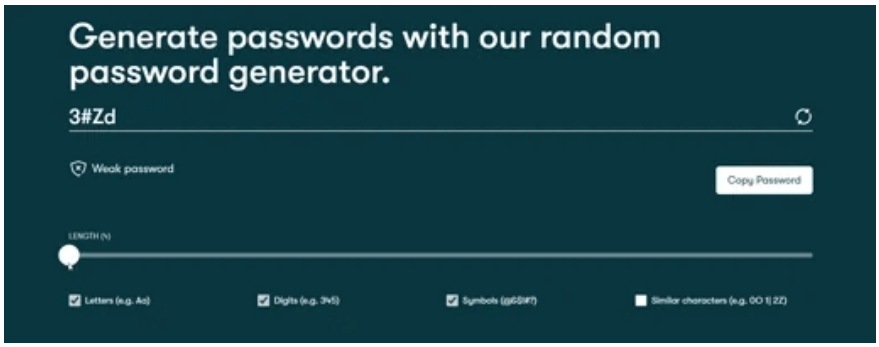
5 Misconceptions About Password Security

These outdated password misconceptions can jeopardize your security, which is why they need to be changed now.

Passwords are the first line of defense against security threats. However, these outdated password misconceptions can compromise your security, which is why they need to be changed now.

Misconception 1: A strong password is enough for everything

If you're using the same password across multiple accounts, you're falling victim to one of the most damaging password security misconceptions. Unfortunately, a strong password isn't enough to keep you safe, and this lack of "variety" can cause more damage than you might realize.



Even the strongest password can be hacked by phishing, brute-force attacks, or keyloggers. If a malicious hacker compromises your login information on one website, the first thing they'll do is use that information to gain access to other websites. Just like that, you've become a victim of cybercrime because you thought coming up with a new password was too much of a hassle.

You can avoid this fate by using different, strong, unique passwords for each account. You don't have to remember them all (or use sticky notes), because you can keep track of your passwords using a password manager.

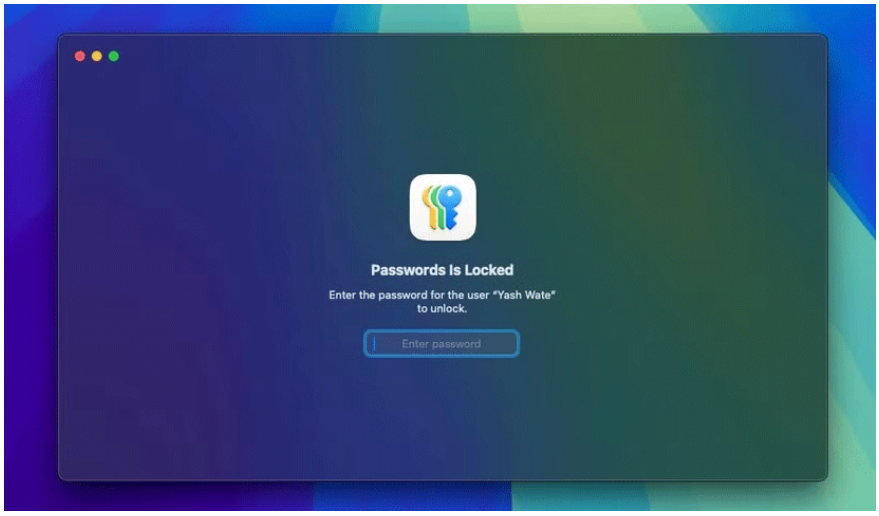
Misconception 2: Passwords are outdated

While new authentication technologies like passcodes may eliminate the overreliance on passwords in the future, it will still be several years before we see a complete paradigm shift.

First, everyone needs to be on board, from website providers to users. While biometrics do enhance security, many still see them as an invasion of privacy. As such, passwords aren't going away anytime soon.

Misconception 3: You should change your password regularly.

If your passwords are already strong and unique, changing them every few months is counterproductive. In addition to making your life harder (since you don't get any tangible benefit from changing them), you may inadvertently create increasingly weaker passwords with each change, especially if you rely on memory.



However, in cases where you've been affected by a data breach, someone has tried to access your account, or you've used an unprotected public Wi-Fi network, you should change your password — just make sure it's as unique and strong as your old one.

Misconception 4: Multi-factor authentication is perfect

While it may seem like it's immune to hacking, multi-factor authentication (MFA) is relatively easy to bypass for skilled and persistent cybercriminals.

For example, they can send multiple authentication requests to a user until they gain access. Phishing has long been effective, with hackers posing as IT support to pressure you into providing your MFA code.

Ultimately, while MFA is certainly a good way to increase your overall security, it's not a foolproof technique that can eliminate every threat.

Misconception 5: Complex passwords are inherently more secure

Think a password with a bunch of random symbols and numbers is impenetrable? Think again!

Sadly, there's nothing you can do about this. A website or company may ask you to increase the complexity of your passwords by implementing specific rules, but they may store them in plain text without encryption, rendering the whole process pointless.

It is also a standard practice for cybercriminals to use certain rules to their advantage. For example, if a website has a minimum and maximum password length requirement, hackers will have a clear starting point and will try combinations that meet these requirements.

Length and complexity are effective defenses against brute-force attacks, but you should also consider the originality of your password. Hackers often use password spraying techniques to crack common passwords across multiple websites. Most security systems block these attacks, so if your password is original, you'll reduce your chances of falling victim to this blind cyberattack.

You finished reading the article "**5 Misconceptions About Password Security**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com