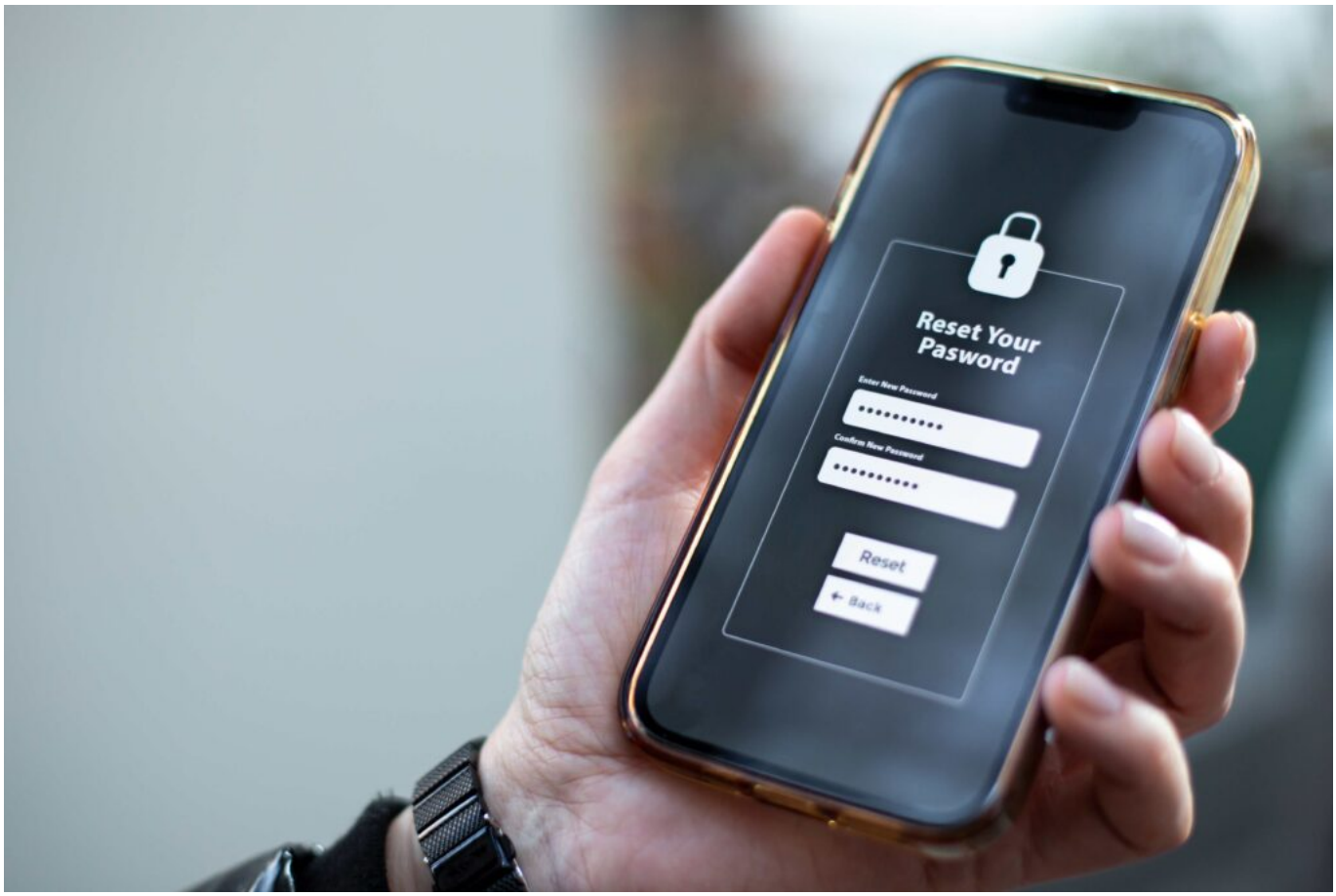
6 tips for creating a secure password.



Frankly speaking, the safest passwords are the ones you can never remember. And that's why today IT experts recommend creating complex passwords that are changed frequently and stored safely. Wondering what steps to take to create more secure passwords for personal and professional accounts? Follow these six tips.

1. **Make them long and complex.** Each additional character in a password increases its complexity exponentially. That's why it's recommended your passwords be at least eight characters in length, but better yet, 16 characters or more with a combination of uppercase letters, lowercase letters, numbers, and symbols. To start, string together three or four random words. Then, make those words more dynamic by adding symbols, numbers, and capitalization. If you need help coming up with a password, use a free password maker online to spark inspiration and tweak it from there.

2. **Don't use personal information.** Things like names, birth dates, address numbers, anniversaries, and initials are common among consumer passwords. Because a lot of this information is public knowledge, it's the first place many hackers turn to when trying to access your accounts. Avoid using obvious selections altogether. In addition, remove specific facts like your birthday, photo of your home address, or pet names from your social media channels so these clues are even less public.

3. **Don't use sequential or repetitive characters.** Steer clear of simple combinations like "ABC" and "123," as these iterations make for a significantly less secure password. The most secure password is a random password.

4. **Use a password manager system.** Most people use the same password for every account simply because it’s easy to remember. But what happens if someone guesses the password you’re using? Suddenly, they know how to log in to many of your accounts and access all your information. To avoid this, experts recommend using different, secure passwords for everything. But we know remembering them can be a tough task to tackle — which is where a password manager comes in. Resources like iCloud Keychain will store your login credentials in its memory bank, so you don’t have to.

5. **Don’t share passwords with other people.** The strongest passwords are stored in your memory or in your password manager, not with anyone else. They’re also definitely not written on a sticky note next to your computer or on a document on your desktop. Run an audit of your personal password storage methods. If you or someone in your life, such as an older adult parent, is storing passwords in a way that’s not secure, start switching to a new method.

6. **If you change passwords, make them different.** Very different. Let’s say you suspect suspicious activity, so you decide to change your password. For safety’s sake, create a completely different one rather than just adding another number or symbol to the end. If systems don’t require timed password updates, set reminders to change your passwords every six months or every year. While changing them may seem like a hassle, it’s far more efficient than having to deal with the aftermath of a hack or breach.

At the end of the day, online security is all about being smart and proactive. These tips will help you make more secure passwords and manage your sensitive accounts and data. Looking for more tools to improve the cyber safety of your family or business? Talk to one of our local, independent agents.