ConnectSafely

QUICK-GUIDE TO

# Secure Passwords

**Is it OK to share passwords?**
Generally, we recommend never giving out your password to anyone. That said, there may be times when sharing passwords could be OK, like helping an aging parent. Another possible exception is young children sharing passwords with parents.

**What makes a strong password?**
Make the password at least 12 characters long. Security experts recommend a "passphrase" rather than simply a password. Such a phrase should be relatively long — perhaps 20 characters or so and consist of seemingly random words strung together along with numbers, symbols and upper and lower case letters. Think of something that you can remember but others couldn't guess, such as YellowChocolate#56CadillacFi$h.

**Any other advice?**
Include numbers, capital letters and symbols. Consider using a $ instead of an S or a 1 instead of an L, or including an & or % — but note that $1ngle is NOT a good password. Password thieves are onto this. But Mbf$TJ1ravng (short for "My best friend Sam T Jones is really a very nice guy) is an excellent password. And this might seem obvious but studies have found that a lot of people post their password on their monitor with a sticky note. Bad idea. If you must write it down, hide the note somewhere where no one can find it.

**Is it OK to use the same password on multiple sites and apps?**
No. If any of your sites are hacked or if a person working at that site steals your password, criminals could try using it on other sites and apps. Vary them at least a little bit by adding unique letters, numbers or symbols for each account.

## What is Multi-Factor Authentication?

Sometimes called two-factor authentication, multi-factor authentication provides another -— often optional — "step" in unlocking an account, device, or document.

Many services, from banking to social media apps, offer multi-factor authentication as an option to provide extra protection for your accounts beyond a strong password. The typical method is to send a text or other type of message to a mobile device registered to you with a code you need to type in to verify it's really you. There are also apps you can use to generate codes. In most cases, you will not be required to use this code when logging on from a known (previously authenticated) device such as your computer, tablet or phone.

We recommend using both a strong password and multi-factor authentication whenever possible.

## More Ways to Stay Safe

**Consider using a password manager.** Programs or web services like RoboForm or LastPass, which work on personal computers and mobile devices, let you create a different, very strong password for each of your sites. Many browsers, including Chrome, Safari, and Edge have free built-in password managers. But you only have to remember one password to access the program or secure site that stores your passwords for you. Make sure that you have a very strong password for your password manager because, if it's breached, it can be used to access all of your accounts.

**Don't fall for "phishing" attacks.** Be very careful before clicking on a link (even if it appears to be from a legitimate site) asking you to log in, change your password or provide any other personal information. It might be legit, or it might be a "phishing" scam where the information you enter goes to a hacker. When in doubt, log on manually by typing what you know to be the site's URL into your browser window.

**Make sure your devices are secure.** Malicious software, including "keyboard loggers" that record all of your keystrokes, has been used to steal passwords and other information. To increase security, make sure you're using up-to-date anti-malware software and that your operating system, apps and browser are up-to-date.

**Use fingerprint or facial recognition for your phone too.** Most phones can be locked so that the only way to use them is to type in a code, typically a string of numbers or maybe a pattern you draw on the screen. Some phones allow you to register fingerprints, which are quite secure. Some apps, especially financial ones, let you open them with a fingerprint or facial scan. (Your fingerprint or facial scan stays on your phone and is not provided to the companies.)

**For more info, visit ConnectSafely.org/passwords**


**Be careful before clicking on a link (even if it appears to be from a legitimate site) asking you to change your password.**

## About ConnectSafely

*ConnectSafely is a Silicon Valley, California-based nonprofit organization dedicated to educating users of connected technology about safety, privacy and security. We publish research-based safety tips, parents' guidebooks, advice, news and commentary on all aspects of tech use and policy.*

Revised 5/18/21