Password Management
Quick Reference for CPAs

Each time you create a password at work, remind yourself how much sensitive client data you have in your care. From names, addresses, dates of birth, and Social Security numbers to tax and financial information, and business entity details—you're tasked with protecting some of your clients' most valuable data. And your network and system security is only as strong as the passwords you create.

Keep this cheat sheet handy to help you create, update, and manage passwords in your practice.

DO

Do use a passphrase instead of a password

Complex passphrases invented from random words are harder for computers to guess and easy for you to memorize, but steer clear of common phrases or popular sayings.

Do change default passwords

If any hardware or software came with a default password, change it! Too many hackers breach systems easily because default passwords were never changed.

Do use multi-factor authentication

Multi-factor authentication using a tool like Google Authenticator is one of the best ways to safeguard systems by requiring you to present something you know (password) and something you possess (authentication code from your mobile device).

Do use a password manager

Use a tool like LastPass, Dashlane, or 1Password, which can generate and store super-complex passwords for you. Make sure to create a strong, memorable passphrase for your password manager.

DON'T

Don't use the same password for all your logins

It may make remembering passwords easier, but it also means that if hackers crack your password once, they can access multiple systems and devices with it.

Don't store passwords in a spreadsheet

Don't do hackers a favor by packaging all your passwords up in a single unencrypted document.

Don't use personal details in your passwords

Don't use any parts of your name, kids' or pets' names, birthday, mailing address, phone numbers, bank PIN numbers, or Social Security numbers in passwords.

Don't use words found in a dictionary

If you're set on passwords instead of passphrases, don't include any real word in English or any other language. Instead, use a hard-to-crack combination of letters, numbers, and symbols.