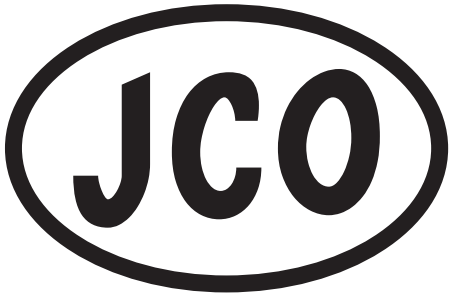


Good Password Hygiene



Think *passphrase*, not just password. The longer your password, errr, passphrase, the harder it is for someone to guess. Or attack using brute force as the case may be. So, use the maximum number of characters a system will allow.

Mix upper and lowercase letters, numbers, punctuation, and other odd characters all together. Use as large a character set as possible when building your password. This makes guess it that much harder. Heck, use multiple languages for that matter. And now keyboard patterns like QWERTY either.

Your password shouldn't have any obvious links or associations back to you. It should be a total surprise when your best friend hears it. So don't use your kids' name, your pets' name, nicknames, license plate number, birthdates, etc. Remember: its a secret. Don't share your secret with anyone else. No one.

Don't let anyone watch you type your password. Same goes try for your PIN at an ATM. Beware of using your password on someone else's computer. Don't walk away from your computer with password-enabled software or accounts still running.

Try using a string made up of the first letters of your favorite song or poem. Mix capitalization too: AscMoSmiTSe

Your password should trigger your spell checker to avoid dictionary attacks. That's when an attacker tries all the words in a dictionary file against your password. If your password is a simply a word eventually it'll be compromised even if it begins with a "z". Make it random, at least without obvious patterns or clues. Try deliberately misspelling a word or

phrase like: kaKewALc

I shouldn't be able to see your password when I'm sitting at your computer. No sticky notes hanging off your monitor or cheatsheets in your top drawer. That's as dumb as hiding a key under the front mat.

Need to share a password with someone? Get three sequentially numbered dollar bills at the bank. New, uncirculated ones. You take the highest, your partner the lowest. The middle serial number is your shared key. Keep yours somewhere OTHER than in your wallet to avoid spending it by mistake.

Need different passwords? Think you have too many? Not rotating them enough? All of the above? Try cataloging your different digital identities: work, personal, anonymous, etc. Use one set of related passwords at work, use another set for your personal email identity, and yet another for your throwaway online personas.

Change your passwords on a regular basis. At least try to isolate the risk if you're compromised and you don't know it. Make the bad guys start all over again. Fight back.

Store your passwords somewhere safe, not taped to your screen. Consider storing floppies and CDs full of passwords (along with software registration numbers and hardware serial numbers, etc.) off-site under lock and key. Perhaps in your safe deposit box. Mail yourself a sealed package and save it unopened using the postmark as an analog date and time stamp.

Take all of this stuff seriously. Hackers and phishers do. Never let your guard down. Actively resist.