

# TIPS FOR STRONG, SECURE PASSWORDS & OTHER AUTHENTICATION TOOLS

*A strong password is your first line of defense against intruders and imposters.*

**Never give out your password to anyone.\*** Never give it to friends, even if they're really good friends. A friend can – maybe even accidentally – pass your password along to others or even become an ex-friend and abuse it.

**Don't just use one password.** It's possible that someone working at a site where you use that password could pass it on or use it to break into your accounts at other sites.

**Newest advice: Use a pass phrase.** Security experts are now recommending a “pass phrase” 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. That's relatively long – perhaps 20 characters or so – using 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. Avoid using famous quotations that might be easy to guess.

**Make the password at least 12 characters long.** The longer the better. Longer passwords are harder for thieves to crack.

**Include numbers, capital letters and symbols.** Consider using a \$ instead of an S or a l instead of an L, or including an & or % – but note that \$!ngle is NOT a good password. Password thieves are onto this. But Mf\$Jlrvng (short for “My friend Sam Jones is really a very nice guy) is an excellent password.

**Don't post it in plain sight.** 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.

**Consider using a password manager.** Programs or web services like RoboForm (Windows only) or Lastpass (Windows and Mac) let you create a different very strong password for each of your sites. But you only have to remember the one password to access the program or secure site that stores your passwords for you.

**Consider using multi-factor authentication.** Many services offer an option to verify your identity if someone logs on to your account from an unrecognized device. 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. In most cases, you will not be required to use this code when logging on from a known device such as your own computer, tablet or phone.

**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.** The best password in the world might not do you any good if someone is looking over your shoulder while you type or if you forget to log out on a cybercafe computer. 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 is up-to-date.

**Use a "password" or fingerprints 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 new phones allow you to register fingerprints, which are quite secure. Sometimes when people with bad intentions find unlocked phones, they use them to steal the owners' information, make a lot of calls, or send texts that look like they're coming from the owner. Someone posing as you could send texts that make it look like you're bullying or harassing someone in your address book with inappropriate images or words.

*\* Some parents ask their kids to share their passwords with them. This might be OK with young children, but you might want to respect your teen's privacy and not ask. Also, if you do ask your children for their passwords, make sure they understand that this is a rare exception to the "do not share password" rule.*