ConnectSafely
Smart Socializing Starts Here™

Tips to Create and Manage Strong Passwords from ConnectSafely.org

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

Never give out your password to anyone (except your parents). Never give it to friends, even if they're really good friends. A friend can – accidentally, we hope – 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.

Never give out your password to anyone (except your parents). Never give it to friends, even if they're really good friends. A friend can – accidentally, we hope – 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.

Create passwords that are easy to remember but hard for others to guess. When possible, use a phrase such as "I started 7th grade at Lincoln Middle School in 2004" and use the initial of each word like this: "Is7gaLMSi2004."

Make the password at least 8 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 1 instead of an L, or including an & or % – but note that $1ngle is NOT a good password. Password thieves are onto this. But Mf$1avng (short for "My friend Sam is a very nice guy) is an excellent password.

Don't use dictionary words: If it's in the dictionary, there is a chance someone will guess it. There's even software that criminals use that can guess words used in dictionaries.

Don't post it in plain site: 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.

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 computer is 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.

Consider a “password” for your phone too. Many phones can be locked so that the only way to use them is to type in a code, typically a string of numbers. 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.