tech TALK

By Pam Simon, MSW

Four Guidelines For Password Management

It is very easy to get overwhelmed and possibly a little paranoid when almost everything we do online now requires at least one, if not more than one, password. From email accounts, playing games and watching videos, to shopping or even making a doctor appointment, the list seems endless! We only have control over our own accounts. Here are a few suggestions to stay safer:

DON'T NAME YOUR COMPUTER STORAGE FILE "PASSWORDS"

According to Common Sense Media, an online resource for digital safety, the number one file name for passwords kept in computers is…Passwords. This mistake has been so prevalent that when Sony Pictures was hacked a couple years ago, it was because their IT Security person had a "passwords" file on his computer. Makes the job of the hacker pretty easy, doesn't it? If you keep a file on your hard drive, call it something else that would be recognizable and significant only to you and or your family. Common Sense Media has wonderful, free "games" about password protection for the whole family to do on their website called, "Digital Passport." https://www.digitalpassport.org

PASSWORD MEMORY APPS

Some people try to keep all their passwords straight in their head. This is virtually impossible and the temptation is to use the same password over and over. The difficulty with that approach is if a hacker figures it out, then he or she will have access to everything. Diversity is how to outsmart the hacker. Even if he or she gets into one account, with multiple passwords, he or she will not infiltrate all your accounts. If you are going to try to remember your passwords yourself, use words or phrases that are meaningful to you, but don't have identifying information like birthdates, street addresses, or phone numbers. All that information is public record and a hacker will guess those things first. There are several password management tools available, to do the work for you. LastPass, Sticky and Keeper are three examples. There are free versions and then upgrades that cost, but might be worth it to stay safe.

LENGTH EQUALS STRENGTH

All the guidance for creating strong passwords point to 10-14 characters in length is ideal. You and/or your children can choose favorite lyrics from songs, lines from books or movies or acronyms. If children participate in the process, they will be more likely to remember the password. It is important to teach children about password security as soon as they start using a computer because it will become part of their daily digital routine. Recently, more and more sites are rating the passwords you enter from "weak to strong." The immediate feedback allows you to adjust the password to strengthen it. The longer the password, the stronger it is against someone else guessing it.

NUMBERS, SYMBOLS AND CAPS

It is highly recommended to include letters, numbers, symbols and capital letters when creating your passwords. If you mix all those characters up, it makes it much more difficult for a hacker to guess and guess right. Therefore, in addition to having a long password, make sure to include a mixture of letters, numbers and symbols. The iKeepSafe Blog on Password Safety and Security provides a wonderful example. The password derives from the sentence, "My daughter, Haley, is a great tennis player." The password becomes, "Md,h,=gr8tP".

There are many, many great resources online to educate yourself about best practice uses of passwords. If you follow these general guidelines, however, you should be in good shape and safer from that lurking hacker!