Passwords - Painful But Important – February 11, 2023

(This is one of a series of articles provided by the Oakmont Technology Learning Center on the use of technology by seniors.)
Tina Nerat and Jeff Neuman

All of us have (too) many passwords: access to our devices (computers, tablets, smartphones), apps, web sites, bank accounts, and more. It is painful to keep track of passwords. Some keep passwords on a piece of paper next to their computer – bad idea! Password managers are available, but some of these have had recent breaches.

So what makes a good password? Each site or app will have their own requirements, but longer is better (at least 12 characters) and words that don't have a natural flow to them. It is best to have both uppercase (A-Z), lowercase (a-z), numbers (0-9), and special characters (e.g. !, &, #, %, or others). The same password should NOT be used on multiple sites or apps. Do not use personal information, such as birthdays or a pet's name as a password. Replacing letters with numbers in a password can help with remembering it.

If you follow the above guidelines and have very good passwords, you should still be secure without periodic password changes. Some sites require passwords to be changed on a regular basis or after a known breach. If you are forced by a web site or app to change a password, do not reuse passwords.

Some possible options on passwords, based on your preferences:

- Use two-factor authentication where possible (text to your cell phone, facial recognition, fingerprints).
- Have an "algorithm" for passwords – a "root" word with numbers and special characters.
- Keep a "paper" book of passwords (don't forget to grab it in an evacuation), but notate the passwords in a "code" known only to you so theft of the book doesn't make passwords readily available.
- Keep your personal details off social media (answering "quizzes").
- Keep an encrypted password-protected electronic spreadsheet of passwords (and important: a backup of it).
- Browsers can also save passwords, but use caution, having your computer or device password- or PIN-protected and be careful with which passwords you want "saved." Anyone on that computer can see the saved passwords.

Think about your digital legacy: who will have access to your passwords when you are incapacitated (see 10/8/2022 article on this subject). Also be aware there is a move to go to "passkeys", a new type of password-less access. An electronic copy of this article, previous articles, as well as more information with clickable links about passwords, password manager data breaches, and passkeys are at oakmont-learning.org under Tech Articles.