THE COMPUTER CORNER

No. 224: Passwords

Stan Kaplan, WB9RQR 715 N. Dries Street Saukville, WI 53080-1664
(262) 268-1949 wb9rqr@att.net

Note the change in my email address above. Please be sure your address book reflects this change. Changes in security at my old address (skaplan@mcw.edu; Medical College of Wisconsin) make both sending and receiving non-business mail more difficult for me. The new address in the masthead above will work fine.

As usual, the ORC breakfast on Saturday mornings provides interesting topics for this publication. This morning (1 October 2016) yielded two. One from Brian Skrentny, (N9LOO) on constructing your own secure passwords. The other from Ed Rate (AA9W) on securely erasing files and folders so that the data is unrecoverable. We'll "do" Brian's suggestion first and save Ed's for next month.

One approach to a secure password is to have a program generate a strong password and then encrypt it (and others) in a vault. You don't have to remember the various passwords you put into the vault. You do have to remember the master password that lets you get into the vault! The encrypted passwords and the master password are all kept on your machine. There are schemes out there that keep your encrypted passwords offline (in the cloud), which turns out to be on some company's server somewhere. I don't recommend that. Keep it on your own machine. Maybe keep a handwritten copy of the master password and the others in your safe deposit box, or in a well-hidden place away from your machine. Don't paste a copy under your keyboard, or on the frame of your computer screen! Anyway, if this is the way you want to go, one of the best around in freeware is found on majorgeeks.com. Go to: www.majorgeeks.com/files/details/lastpass.html to see and download the latest version of LastPass, a general password manager. Its writer claims you can "generate strong passwords, knowing you'll only have to remember one, log into your favorite websites with one click, access and manage your important data from multiple workstations seamlessly" and more. This might be what you want to handle the passwords, once you have them. But let's consider what a strong password might be, and why strength might be important.

Gone are the days when a four-character password (ABCD, 4321, 24SK, 24sk, etc.) would do. Crackers can crack one of these in seconds, not minutes, using a just a home computer! So just a four, five or even a six-digit password will no longer do. Really strong passwords today consist of at least ten to a dozen characters, and as you have heard somewhere, the characters need to be a mix of digits, uppercase letters, lowercase letters and punctuation or other characters such as %, $, # and so on. On the other hand, at breakfast today, Brian pointed out that length is more important than complexity. He also gave us a really good example. He uses something like this: **I paid $32.02 for this shirt today.**

This example an intelligent phrase in perfectly good English, using 35 characters. It uses caps (the very first character) and lower case letters, punctuation marks and other characters ($, the decimal point, the spaces between words, and the period at the end), and digits (in the cost), so all the elements are there. Moreover, if you associate it with your favorite shirt, your new car, your new HT, you will not be likely to forget it. And it is strong. Brian says it would take years to crack with a supercomputer, and this is Brian's business.

So before you even start messing with a password manager, why don't you create something like Brian did, and use that here and there when necessary. Most email clients and browsers have a password manager built in and will save your choice on your computer for use on line, if you wish. And with that, let me leave you with a strong password: **Happy Computing for the 224th time!**