Welcome to Securing Your Digital Footprint-

Passwords/Authentication-

Everything starts with passwords, they are the first best defense in our security battle. In the beginning of our use of passwords, they were short and usually pretty easy to guess. But as we have matured we have continued to make the passwords more complex - harder for humans to remember and easier for machines to crack.

Passwords of today have been replaced with a passphrase. This is a phrase that is a combination of upper and lower case, symbols and numbers and is at least fourteen characters. The key is to have something like: 1mG01nG2tHeZ00#. Don't use something that is specific to you, like birthdays, anniversaries, relative's, pet's names. NEVER, NEVER, Never use a passphrase for more than one site. If the Bad Guys crack one website, and you've used that same password for others… (Game Over)

Before you go to the trouble to come up with passphrases, verify they aren't already out there, released in any data dumps. We used to say, change your passwords, yes all of them, at a minimum of every three months. Now the thinking is not to change them unless there has been a breach/hack.

With all of the characters needed for one password how are we supposed to remember that, let alone dozens? Password managers/safe - allow for the storage of all passwords needed to access our digital life. Have you ever typed in a password in your browser and had a popup window ask if you want to save it? That is a password safe at work. Windows/PC does not come with one, but Lastpass and 1password are good choices. Apple comes with Keychain. Make sure you create a very strong master password for your safe - write it down and keep it secure. Yes, I did say write it down, what's old is new again, when it comes to keeping passwords secure. Verify that the master password to get into your password safe/manager is very strong. One of the new hacker attacks is to go after that password. Alarm bells went off, when I recently heard someone keeping the password for his password safe/manager on Dropbox. Putting something so valuable onto a not so secure cloud seems foolhardy to me. Your mileage may vary.

Trying to come up with passphrase can be a bit of a challenge - luckily there are password generators. You set the criteria, it creates your passphrase. Most password manager/safes come with one of these useful tools. To truly be secure you should be using Diceware, unfortunately not many password generators use them at this time.

Passphrases created, password safes setup, time to move on to two-step-authentication (2FA). The next barrier to stop hackers breaking into your accounts. 2FA confirms your identity through a combo of two different components; for example an ATM requires both a bank card (a token or artifact the user possesses) and a PIN (something that the user knows) before greenlighting a transaction. 2FA

can send a text, phone call or email to verify that you are who you say you are. This stumps the hackers as they don't hopefully have access to those methods.

If you get a 2FA notification and you aren't in the process of logging in to an account, don't respond, but make a note of what account is trying to be accessed. Open the website for that account DON'T login, but find the fraud dept. or send an email to them explaining what happened.

That wasn't so hard, you should be feeling confident with your new skill set and added knowledge. Let's continue to build on that, as we move on to the least secure form of communications in our world today.