**WTF is my Password?**

***Not everyone has problems with remembering Passwords, but some of us do (including Me).***

**These** are not normal times – for many reasons. But regardless of what’s happening in Russia, China, or Ukraine, most of us are required to remember a number of passwords, that must be changed for any number of reasons. This is the problem, we should not use passwords than can easily be guessed by hackers. If you are a target of a hacker, the hacker probably knows you, or knows something about you and that is why you have been targeted.

Our Passwords are our first defense to prevent any hacker from interfering with our use of our digital devices. **BUT**, many of us need more than a few different passwords for our ATMs, access to our bank accounts, to department stores, access to our stock trading accounts, access to Eventbright, to many websites we used regularly, and our email accounts that can reveal everything about us. So most of us, who do not have photographic memories are in a lot of trouble these days. Most of us must know at least a dozen Passwords, and some of us have 20 or more different Passwords to conduct the business of life in the 21st Century.

Passwords are unavoidable and a curse most of us live with every day. Are there any secrets or techniques that can help us create new passwords or change existing Passwords? One simple, but one which requires some discipline is having a ledger for our Passwords. These can be purchased on line for less than $10.00. We will have a few for door prizes at our next post meeting. Bring at least $5 to our next Post meeting for a raffle and a chance to win a Password Passbook. Afterwards, you might be able to sell your prize for double the cost of a raffle ticket.

The first headache we have when dealing with creating or changing Passwords is complexity. We will be reminded that the Password cannot be too short, most of the time we need to have 8 characters and they must include at least one capital letter and at least one number. Often e must also include one symbol like an **!** or **#.**

We are all human beings, so strings of letters, numbers and symbols are too difficult to remember - if we must remember more than a few nonsense strings of characters. Some entities offer us the opportunity to have an extremely complex Password that most hackers will not be able to unscramble. But if a hacker finds out your ID, your birthdate, cell phone number, or your home address, they might be able to get entry to whatever entity/organization retains your super complex Password.

So what can you and I do, to create dozens of our own Passwords that you and I can remember, but is too hard for even friends to figure out our secret Passwords.

The following is quoted from the article “What’s Wrong With Having “Complex” Passwords? A Lot.” Karen Renaud, WSJ, September 9, 2021, R10

**QUOTE:**

“the best passwords are those that are composed of interconnected parts.

In essence, this would be a passphrase, composed of at least three different words. Not coincidentally, that’s the kind of password that the organizations mentioned above recommended in 2017.

If people use three or more words as their password, they can memorize it more easily, tailor it to the specific account the password is being used for, and then not have to write it down. For example, consider the relative difficulty of memorizing “Ih&Kdxp!” vs. “Rhinos are scarcer than Yellow Jackets.” The latter is much easier to recall. It could, say, be your password for the account you have at the local zoo. Or “Good Health Is Peachyl” could be your passphrase for your company-benefits site. Adding humor enhances memorability.

Recent research suggests users can strengthen passwords even more by using two different languages in a single password. So instead of “Rhinos are scarcer than Yellow Jackets,” you could use, “Rhinos are scarcer than Gelb Jackets, using the German word for “yellow.” That’s still easy to remember, but so much harder for hackers to guess.

In other words, instead of trying to tell people to eschew complexity requirements, and risk triggering a resistance to change, we could point out that passphrases are just another way to meet complexity requirements, too. And a lot easier to remember. “

**UNQUOTE**

So this one solution for helping many of us to deal with the curse of Passwords. LOL.