# CS CYBER SECURITY & YOU

AUGUST 2019

## HOW DO I CREATE A STRONG PASSWORD?

To answer this, we must first define what makes a password strong. The characteristics in order of importance are:

**1) Length, the longer the better.**

**2) A mix of uppercase, lowercase, numbers, and special characters.**

**3) No personal information.**

**4) No proper names or dictionary words.**

There are many ways to invent a secure password. One way is to first start by finding a base set of characters. Some start with the acronym of easy to remember phrases or quotes; like "if the shoe fits, wear it" which yields "itsfwi." Others misspell words intentionally; like blue becomes "bloo" or true becomes "troo."

Okay, we are off to a great start, but rules 1 and 2 have not been applied. We can pad the length of the 1st example with numbers and special characters, and change a couple of the letters to uppercase. The nouns can be changed to uppercase and the comma added back in so we get "itSf,wI." Adding a random special character and number result in our first example password "*itSf,wI6." This is a little hard to remember!

Was this too hard? How about using our second example with a smiley face ":^)?" "trooBLOO:^)". This would work as a strong password and is easier to remember, but we can do better.

One last and even easier way is to use a passphrase, or a sentence instead of a jumble of characters. For example: "It would hurt to fall down 10 stairs!" or "I owe Joe $44 for the bow." Of the three password types, this is the strongest, simply because of the length (even though it breaks rule #4) and is often the easiest to remember.

### QUICK TIP

There are tools on the internet that will help you determine the true strength of a password. One that I use is from LastPass and can be found here. Never type your real password in any of these sites, but instead use comparable passwords (the same numbers of each type of character). By experimenting with these tools, you can understand what is required to create strong passwords.

## WHY DID WE INCREASE THE REQUIRED LENGTH OF OUR PASSWORDS FROM 6 TO 8?

As computers get faster, the amount of time required to guess passwords decreases. This chart describes the amount of time required to guess a password:

| Password length | Time for a computer to guess | Projected time for a computer to guess 10 years from now |
|---|---|---|
| 7 | 11 days, 14 hours | 2 hours, 46 minutes |
| 8 | 2 years, 139 days | 8 days, 16 hours |
| 9 | 178 years, 207 days | 1 year, 286 days |
| 10 | 13,392 years | 133 years, 388 days |

LASERS IT
Making Digital Retirement a Reality