LONG PASSWORDS OR COMPLEX PASSWORDS – WHICH ARE STRONGER?

Passwords are still the most common form of access. Even though other methods are stronger.

Making matters worse is the number of passwords needed to access all the devices, systems, and applications. Remembering them all is virtually impossible.

What are the options? Write them down? Often done. Use the same or similar ones for different things? Also done.

So, what is the answer to keeping things secure? Sadly, the answer is, it depends. Long passwords tend to be more secure than shorter ones. But not if people pick common words or phrases that can be easily guessed.

Cracking a password falls to tools these days that try common phrases and words first. Which are also what people find the easiest to remember. The second step is to try every possible combination. But this takes time and compute resources.

But are complex passwords the answer? Complex passwords use upper and lower case, special characters, and numbers. That set offers 96 possible choices for every position in the password.

Taking a simple example, if the password is one character long, and only numbers are used then there are 10 possible choices. If the full character set of numbers, upper- and lower-case letters, and special characters are used, then the possible choices are 96.

Since 96 is greater than 10, it seems the full character set is much more secure. However, if we add one more digit to the numbers only version, that provides 100 possibilities or about the same as the single complex character password.

Complex passwords are more secure than simple ones. But as the example above shows, doubling the number of digits provides the same level of security as a complex password.

Using brute force to crack a password means trying every possible combination. And this takes time and resources. Another example. Think of the combination locks used for school or gym lockers. Many have 40 numbers on the dial and three numbers in the combination. 40 times 40 times 40 equals 64,000 possible combinations. It would take someone a long time to try them all and anyone watching would get suspicious.

But what if they had a “bionic” hand and could try 1000 combinations a second. Then 64,000 would only take 64 seconds. The combination locks would no longer be an effective way to secure things. That is the downside of faster computers. The new quantum computers would be like the “bionic” hand and render almost all password-based security useless.

But until then, longer passwords with upper and lower case, numbers, and special characters that aren’t a familiar phrase are the more effective means.

To learn more about cyber protection and education contact Aurora Information Management at info@AIMglb.com or call (888) 773-1920.