CS

CYBER SECURITY & YOU

DECEMBER 2020

Tips for Creating STRONG PASSWORDS

As mentioned, there are sophisticated hacks and simple hacks but one constant - poor username and password policies and knowledge. Here are the top tips for creating strong passwords.

1 USE PASSWORDS WITH AT LEAST 10 CHARACTERS

Your passwords should contain at least 10 characters. I know, it sounds like a lot. Long-tail, complex passwords really are hard to crack. To make your passwords complex but memorable, utilize several types of characters, a mixture of lower and uppercase letters, and symbols.

2 DON'T USE PERSONAL INFORMATION IN YOUR PASSWORDS

You should avoid using personal information as these are the first options that hackers try to exploit. Hackers attempting to hack your accounts might already know personal details like your address, street, phone number, spouse's name, children's names, pet's name, birthdays, anniversaries, and so on. They'll use that information as an aid to guess your password more easily.

3 DON'T USE COMMONLY USED PASSWORDS

This is one of the biggest mistakes you can use with your password. Don't use common passwords like "password" or "123456." These are some of the easiest passwords to hack and can lead to a serious data breach or access to important accounts.

4 DON'T USE COMMON DICTIONARY WORDS

This is a really tough one to put in place, but you should avoid using common dictionary words. Using common dictionary words are often used in brute force attacks. In addition, using two common dictionary words does not make your password more secure against an attack. For example, do not use "Red," "Cars," or "RedCars." It's actually better to misspell or make up words if you can. Instead, use something like "RedddCarzz." You would also want to add some other character types to it as well.

5 USE COMPLEX PASSWORDS WITH SPECIAL CHARACTERS

I mentioned that you shouldn't use common dictionary words. The next step is to add more complexity by adding special characters. This includes replacing letters with numbers and punctuation. Here are some ideas to help you create highly-complex, unusually spelled, and unique passwords.

TotallySecurePasswords! = T0ttallySecur3Pa55w0rd5!

BeyondComplexPass# = B3yondc0mp1exPa$$#

It's that easy. Use a phrase or word and then mix it with shortcuts, nicknames, and acronyms. Using shortcuts, abbreviations, upper and lower case letters deliver simple to remember, but protected passwords.

6 USE AN EASY TO REMEMBER PHRASE

It's really frustrating when you cannot remember your password. One alternative is to create a phrase and then mix it up by shortening it, adding nicknames, misspellings, and acronyms. This will deliver a password that is easy to remember, but safe. Here is an example:

Use something that you would only know, such as one of your college house addresses and how much you paid in rent, or when you graduated.

CollegeRoodStHouse$750 = C0llegeR00dStHouse$750$

Make sure to mix up the words.

7 USE DIFFERENT PASSWORDS FOR DIFFERENT ACCOUNTS

You should use different passwords for different accounts. I know, it seems like a pain, but if you are using the same password across many accounts and your credentials are compromised, all of your accounts using those credentials are now vulnerable.

8 USE PASSWORD GENERATOR AND MANAGER TOOL

Implementing strong password policies as well as training and enforcing them is a difficult task for all businesses regardless of size. With a large number of websites and accounts we access on a daily basis, there's no logical way to remember different passwords for each account. Further, writing them down or storing them can be yet another security risk.

A password manager can help your users generate strong passwords in addition to remembering them. Instead of remembering 15-20 passwords, your users will have to remember a single root password. Now, you have to remember that a strong root password and 2FA will be critical; otherwise, hackers could potentially hack your password manager tool.

9 USE TWO FACTOR AUTHENTICATION

This is one of the most important password protection strategies you can have. What is two-factor authentication? Two-factor authentication, also called 2FA, is a two-step verification procedure, or TFA. It takes more than a username and password, but also something which only that user has on them.

For example, after entering your username and password, you may have to further verify by using an email, phone, or 2FA code generator. This adds an additional level of security and alerts users to potential hacking attempts.