Choosing a Strong Password

We have seen it all over the news; incidents of password reuse are on the rise. Hackers have obtained usernames and passwords leaked from websites such as LinkedIn, Facebook, Instagram, etc.... Even Mark Zuckerberg, Facebook's CEO was hacked. It is for this reason that passwords are often considered the weakest link in the cyber security ecosystem.

What is password reuse?

Password reuse is when people use the same passwords for accessing all their online accounts and profiles. Using the same password greatly increases the chances that hackers or fraudsters can access your personal, private, and or corporate data- exactly what hackers or looking for! Security experts all agree password reuse is a huge detriment to digital security.

Why should you use different passwords?

Using the same password for all your accounts is like having one key that unlocks every door in your life. It would be extremely unwise for a person to rely upon one key to unlock their home, their car, their office, and their safe deposit box because if that key were to get lost it would simultaneously create multiple high-risk situations that would need to be addressed quickly.

The same principle applies when people use the same password for their email, bank account, credit cards, streaming sites, and social media accounts. If you use the same login credentials across the internet, then it won't take long for a savvy hacker to identify multiple places they can use your stolen password.

So, how do we choose a strong password?

First, you must make sure you don't fall into the common password pitfalls. There is a joke on the internet that says; "I changed my password to "incorrect" so whenever I forget it the computer will say, "Your password is incorrect". It is a funny idea but protecting your password is a very serious matter.

ASK YOURSELF: What do you think are the most common mistakes we make when choosing a password?

ANSWER:

- Too Short
- Too Simple
- Using the same password
- Writing passwords down

Too Short: A decade ago a five-character password was more than a match for the average computer. As tech has advanced so have the fraudsters and their methods for defrauding our customers and us. When making a new password, eight characters should be the absolute minimum, ten to twelve characters is recommended. Some experts in the IT industry commonly use and recommend thirty-character passwords for systems.

Too Simple: Even twelve-character passwords aren't going to do much good if it's as simple as "1234567892017" or "Password123!" Hackers check for those things right away. A strong password will have a mix of upper- and lower-case characters along with numbers and symbols.

Using the Same Password: The importance of creating unique passwords for all of your various online accounts is recommended that way, if hackers do access one of your passwords, they won't gain access to all your accounts.

Writing Passwords Down: Don't undo the strength of your password by leaving it written down on a Post-it note near your laptop or desk. Don't record passwords in a notebook either. If a fraudster is paying close attention notebooks and notes will be easily spotted.

Examples of simple words that can become good, complex passwords.

Password – P@55w0rd
Something – S0m3Th1n6

Even adding: !@#$%^&*()~ to plain text passwords make them even more complex than people think.

Using mixed cases along with numbers and symbols goes a long way to secure your information.