Computer-Ease
Complete Computer Solutions
www.CVWare.com

Custom Programming IT Services Network Management Websites Computers

A Strong Password is Your Security “Super Power”

“Love ’em, hate ’em; don’t really think about ’em.” These are some of the comments I hear over and over again from clients when I bring up the importance of creating strong passwords for your electronic devices and the internet. Whether it’s a password for your computer, cell phone, tablet, or a website, the fact is that a strong password is the most powerful Cybersecurity “super power” you possess to protect your information, your identity, and your money from hackers.

Realizing that a good antivirus, proper email security, and a good understanding of what to do and what not to do when surfing the internet are all pieces of the security system that you must utilize, and strong, unique passwords provide the foundation for your safety.

Unfortunately, it’s also a fact that one of the worst things you can do to make your valuables vulnerable to an attack is to use weak passwords.

Today, I’m going to show you the exact method to create strong passwords that will help safeguard your devices and internet accounts from hackers and why you need to use it.

Do you do any of these things on your computer or phone?

- Pay a utility bill online.
- Write and send an email.
- Store family photos on your hard drive.
- Order merchandise at an online store.
- Signed-in to a favorite website.

If you do just one of these activities with your device and use a “weak” password, you have created a serious Cybersecurity risk to yourself and your valuables.

But what exactly makes a password “weak”?
A weak password is one that:

1. **Is too short**. This means that the number of characters in the password is so low that its easy to be rapidly found and “cracked” by hackers.
2. **Is commonly used**. This means too many people use this password and it is already known.
3. **Has information about your life**. This means the password includes some information that is easily guessed, looked up or known, such as: your name, your pet’s name; yours or a family member’s birth date, address, or anniversary (*or anything similar)*.
4. **Doesn’t contain enough character combinations**. Characters are not enough, you need numbers, upper AND lower case characters and then special characters.

Passwords with these weaknesses make them extremely vulnerable to “bad actors” who want to hack, steal, and sell what belongs to you, and using them can lead to being hacked in just a few seconds!

According to recent articles on CNBC, NordPass VPN and CyberNews, compiled lists of passwords from data breaches and password lists for sale on the dark web, show that the current most commonly used passwords are: **“password,” “password123,” “123456,”** or a derivative of them. These and the passwords listed below are the easiest and fastest to hack and steal. (And a*ll of these take less than one second to hack.*).

Research conducted by NordPass VPN shows a few more examples of really bad passwords:

- **123456 –** and statistics show over 103 MILLION people use it!
- **123456789 –** and 46 million people use it!
- **qwerty123 –** and 12 million people use it!
- **abc123 –** and more than 10 million people use it!

Today’s hackers have access to increasingly high-powered computers that provide them with the ability to “Brute Force Attack” with *trillions* of password combination attempts per second, so even passwords like these are quickly hacked:

- **MyPass2** hacked in thirty-six seconds
- **MyPass22** hacked in seven minutes
- **SecureIt21** hacked in two hours.

Awareness of what a weak password is and how dangerous it can be to use one is key to protecting your valuables.

So, then what exactly IS a “strong” password?

A strong password is one that is “long enough” and contains enough different characters that it cannot be easily guessed or hacked using either a “Bruce Force Attack” or a “Dictionary Attack”. (A dictionary attack uses whole words found in the dictionary to test and guess your password.)

A “strong” password contains all of the following:

1. **The longer the better**. You should use a minimum of 12 characters. (20 characters is better, 32 characters is even better, and really strong security is up past 64 characters even.)
2. **Randomly selected words; or better yet – partial words**. If you use words in your passwords, they should be random or partial words, and have nothing to do with the ‘purpose of the password’ or yourself. (by ‘purpose’ I mean for a Bank of America password you should never have anything that is related to the name – ie. Bank or BofA etc.)
3. **Both upper and lower case characters**.
4. **At least two or more numbers**.
5. **Punctuation marks or special characters**. Special characters include: # $ @ ! , & ^ % . as well as others.

And some additional steps to keep your password strong, you should also:

- Make sure it has nothing to do with you, your kids, animals, birth dates, or contain any other information that is commonly known or could be found out about you. (remember, social media may very well contain much of that information already!)
- Make sure that passwords are changed at least once every year (every three-to-six months is even better!)
- Make sure the password is NEVER reused at any other website or on any other device

To sum it all up, creating a password consisting of 12 or more characters, partial, random words, and tossing in some numbers and at least two special characters is an excellent method to make a password strong and secure.

And the time it takes to crack a password built with these rules, proves the reason you should use it.

Some examples of strong passwords:

- **MobiPrka#423!** - 11 million years to crack
- **Baskt.21@Crik2!** - 2 trillion years to crack
- **Guitr71.IsBettr2$** - 16 quadrillion years to crack

Reusing Passwords

OK, you now have a GREAT method to make strong passwords, and you've created a strong password that you REALLY like. In fact, you like it so much you might be thinking that you want to reuse it everywhere. Nope! **NEVER!** And here's why: Every time a website is hacked, one thing the bad actors attempt to collect are email addresses and their passwords; these are the "keys" that unlock *your valuables, not only at that website, but anywhere you reused this combination!*

And the bad guys sell passwords lists! If the bad guys get a hold of that list of email addresses and passwords, you can believe that after they have attempted to use that list to "hack some websites", that list WILL end up for sale on the dark web.

Best practice: NEVER reuse a password!

Keeping Track of that password

Now that you have the method and rules for passwords, several more things become obvious. First and foremost, if your passwords are really good ones, you are NOT going to remember them all, so you have to save and store them. That means finding the right password when you need it; making sure you have the most current password; and keeping any previous passwords. (even the weak ones) Keeping a list of previous passwords as you change them, could help you if you need to recover an account.

That little book you write your passwords in is good, but it's not really simple to use, not really safe, nor easily updated. Using a P**assword Manager** is a great way to safely and securely keep ALL of your passwords in one place, making it easy to find and use when you need them. It also is an excellent way to update, track old passwords and even save and keep security questions, and much more.

In the next article I shall discuss more about why and how to use my **recommended password manager, KeesPass**. I believe KeePass is a perfect solution to maintaining passwords, securing other important files and data, and it's free!