I know we've beaten this topic to death, but it's a quick read and a gentle reminder to reevaluate your passwords.

By Kim Komando... USA Today

There's a joke going around the Internet that says, "I changed my password to 'incorrect' so whenever I forget it the computer will say, 'Your password is incorrect.'" It's a funny idea, but passwords are actually a serious matter. They're often the only thing standing between a snoop and your information or money.

Today we're going to go over the most common password mistakes you can make, so you know what not to do. I'll also share some easy ways to make creating and keeping track of passwords less annoying.

1. TOO SHORT

A DECADE AGO, A FIVE- OR SIX-CHARACTER PASSWORD WAS MORE THAN A MATCH FOR THE AVERAGE COMPUTER. HOWEVER, COMPUTERS HAVE INCREASED IN PROCESSING SPEED AT SUCH AN ASTOUNDING RATE THAT A SIX-CHARACTER PASSWORD IS AS BAD AS HAVING NO PASSWORD AT ALL.

When you're making new passwords, 8 characters should be the absolute minimum, and 10 to 12 characters is recommended. For super important accounts, such as your banking account, a 14 to 16 character password isn't a bad idea. My I.T. staff uses 30-character passwords for the important systems.

2. TOO SIMPLE

Even a 12-character password isn't going to do much good if it's something as simple as "123456789012" or "abcdefghijkl". Hackers check for things like that right away.

Even a common phrase like "maytheforcebewithyou" is something hackers look for right off the bat. They have dictionaries with millions of the most common passwords and variations, and they can crack these simple ones in minutes or even seconds using home computers.

A strong password needs to have a mix of upper-case and lower-case characters, along with numbers and symbols. However, you can't just get away with simple substitutions like "Mayth3F0rc3Bw!thU!"

Something like that will slow a hacker down, but modern computers are fast enough to try substitutions like this as well. Your password needs to be virtually random.

Instead of just randomly hitting keyboard keys, however, try another method that makes the password easier to remember. Start by thinking up a random sentence. You can use a catch phrase, quote or even a song lyric like "Tramps like us, baby we were born to run."

Take the first character from each word to get "tlu,bwwbtr". Add some symbols in place of similar letters, so "u" becomes |_|, the "to" from the original lyric becomes 2. Then, capitalized a few of the letters to make a strong password that's easier to remember than a random password: "Tl|_|,BwwB2R".

However, when you have dozens of passwords, remembering them is going to be a problem even with this method. That's why you need to keep in mind the next two mistakes.

3. NOT UNIQUE

As passwords get longer and more complex, it's tempting to use the same password for every account so you only have to remember one. Unfortunately, if you do this and a hacker gets a hold of your password for one account, say in a data breach, they can log into all your accounts.

You need to create unique passwords for every account you have. Of course, that makes it really hard to remember your passwords, which leads to mistake number 4.

4. WRITING PASSWORDS DOWN

Many people create strong, unique passwords and then write them down on sticky notes that they stick on their desk. Some people keep their passwords in a notebook that they leave lying around.

A hacker won't have much of a chance of seeing those, but what about snooping family members or friends? Maybe your house is robbed and burglars end up with your password notebook. If the burglars are smart enough they can cause you a lot of trouble.

Instead of writing the passwords on a notebook, get a password manager. This is a program that stores and locks your passwords behind a single Master Password. You can create dozens of strong unique passwords and only need to remember a single password (and you can use our formula in point 2 to make it).

Some popular password managers include free ones like KeePass and Kaspersky Password Manager(full disclosure: Kaspersky Lab is a sponsor of The Kim Komando Show).

Many of us in BCTC use LASTPASS, also free.

5. NEVER CHANGING PASSWORDS

You might have heard the recommendation that you change your password every 6 months, 3 months or even monthly. However, the Federal Trade Commission recently did a study that shows you shouldn't regularly change your password.

Regularly changing passwords is annoying, which leads to people making passwords too simple or reusing them. In fact, people who regularly change their passwords make them 46% easier to guess. In general, you should only change your password if you think it's been involved in a data breach.

That being said, you should take some time to look through your passwords and update the ones you haven't changed in years. They probably include some of the mistakes above, and you want them to be as strong as possible.

BONUS: POOR SECURITY QUESTION

Most websites have options for recovering a forgotten password, and one of the most common ways to do this is answering a security question you set up in advance. Unfortunately, most security questions are things a hacker or relative can figure out with little effort, such as a mother's maiden name or the street where you grew up.

A weak security question can render the strongest password completely useless.

As another bonus, you should know that many online accounts have a bit of extra security you might not be using. It's called two-factor authentication, and when it's turned on, hackers can't get into your account even if they know your password.