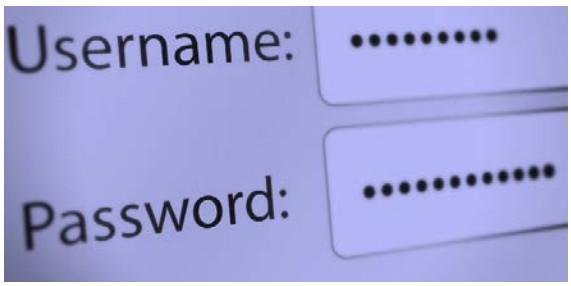
Top 8 Common Password Mistakes and How to Avoid Making Them

No one likes passwords, but passwords are more important today than they have ever been. If you have been using the same type of password for years, it is probably useless today. If your important online accounts; banking, investments, health records or any other critical personal information is at stake, you need to be confident that you are using a secure, random code that a machine can't guess. So, are you ready to reset all of your passwords? Well, not yet, you first need to read through this list of the eight common mistakes to ensure when you reset your passwords you are creating passwords that are secure.

1. Are you planning on using personal information to help you remember your passwords? DON'T!

When you use names of relatives, celebrities, sports teams, pet or any other common terms in your passwords you are setting yourself up to have your password hacked. Criminals use software that automatically looks for the most common combinations like Raiders123. And don't think that you'll be safe if you use personal information like the name of your pet or your even your high school mascot. With social networks, it is simple for criminals to harvest that information that you so innocently post.



And oh, by the way, just adding a string of numbers to then end or the beginning doesn't make the password any more secure.

2. Are you planning on using the same password everywhere? DON'T!

While it is the easiest way to remember your password by using the same one everywhere, you are asking for trouble. Every day criminals send out phishing attacks to capture that password. Studies have shown that nearly 97% of people can't detect a phishing email, so once you provide them with your password, if you use the same one everywhere, they have the info to access all of your accounts and could destroy you financially.

3. Do you use recognizable key-stroke patterns? STOP!

"qw3rty" may seem like a strong password to guess until you look down at your keyboard and notice the easy pattern. In order for a password to be considered random, it must be truly random.

4. Are you using passwords that are too short? DON'T!

Ten years ago you could get away with using a six-character password and it was considered fairly secure, but technology and cyber-criminals have evolved and now that a six-character

password can be guessed by a fairly simple software program attack. Today, a minimum of 12-characters is considered a secure password. Start thinking "passphrase" rather than password.

5. Do you substitute numbers for letters? BE CAREFUL!

While this used to be an effective technique, these days "$afe1y" won't survive a determined attack any. Unfortunately, cyber-criminals and the software the use is on to that trick.

6. Do you change passwords with a single character or number? STOP!

This is a change a lot of people will implement when asked to change their passwords; they comply by changing an "8" to a "9." Password-guessing programs know this trick and will discover it in seconds.

Another variation of this practice is to include a symbol, by adding a "!" or "&" onto the end of your existing pass-word. That's virtually the same as adding a number at the end, and this too will be easily cracked. Non-alphanumeric characters should be used within the password only - not at the beginning or end of it.

7. Do you share passwords with others? STOP!

Even if you have created the strongest password in the world if you share it with someone who stores it in an email account protected by "password1," it won't make any difference at all. Your passwords should NEVER be shared.

8. Do you store passwords in plain text? STOP!

A common and easy way to remember passwords is to store them in a spreadsheet or mail them to yourself. Bad idea. Have you heard of ransomware? It's the fastest-growing category of malware. Cyber-criminals hold your data hostage by encrypting it until you pay them a ransom. Sometimes you get your data back and sometimes you don't. In the meantime, they are searching your hard drive looking for anything that resembles a password list. Once they find it, the ransom payment is the least of your problems.

Your best bet for a secure password is to use a password manager protected by strong encryption. The best password managers will generate secure passwords for you and give you total protection with two-factor authentication.

ITS Technology Simplified

To learn more about password management and how to protect your business, contact ITS.

805-520-7020
www.itstelecom.com