PRACTICING SAFE PASSWORD MANAGEMENT IN YOUR BUSINESS

1stcs.it

PRACTICING SAFE PASSWORD MANAGEMENT IN YOUR BUSINESS

Have you ever seen or experienced this (or are you one of the guilty ones)!?...

Walking around an office, there's something on someone's monitor. It's a Post-It note... and it contains their password.

We've seen this too many times!

Yes, we all have a few problems remembering passwords. But keeping passwords secret is literally the most basic IT security requirement.

Now, I'm not worried that your cleaner is going to start hacking your accounts when you've left the office for the day. But it does make it more likely that you'll suffer a data breach.

Get our top tips on safe password management in this guide.

TOP TIPS FOR PASSWORD SAFETY

1 Your passwords should all be long, randomly generated, and impossible to guess. That means steering clear of children's names, maiden names, birth places, car models or anything else that *could* be guessed.

2 Your password is best held in a password manager, so you don't need to remember them or even type them in (for example, LastPass)

3 Multi-factor authentication is a very useful practice and adds another layer of security. This is where you generate a login code on a second device.

4 Do not reveal your password to anyone else. It is yours and yours alone.

The fact is, hackers know their stuff, and the less complex and short your password, the easier it will be for them. Password hacking is responsible for a considerable amount of cyber-crime.

The 1st Computer Services Way: Use Pass Phrases over Passwords.

Instead of using a random word, and a random set of numbers and special characters, opt for a short phrase.

Examples
- Instead of Notebook123, how about myn1cenoteb0ok1#
- Instead of Mercedes2021, how about IDoL0veMerced3s!

As a general rule of thumb, do try and get over the 10-character mark.

Now let's face another issue that many are guilty of with passwords >>>

Are you using the same password for all of your logins?

This opens up a whole new level cyber-security issues. If one of your passwords is stolen, then those hackers can quite easily get into all of your other accounts.

Think about this... what would it mean to you if a hacker was able to access EVERYTHING that had that one password?

The consequences are not nice to think about, right?

ACTION:

Start now, make a list of all of the actions you need to take to ensure you cannot be hacked due to simplistic passwords.

If you would like support with implementing a robust password strategy within your business, get in touch with our expert team.

1stcs.it

Contact Us

hello@1stcomputerservices.com
t: 01329 630018