TJMicro Tech Tips

Is Your Password Secure?

Technology has transformed how we connect with each other, grocery shop, and pick out our new favourite sweater. It has allowed us to access and complete tasks in ways we could never imagine before. However, to quote Spiderman, with great power comes great responsibility. Each of the accounts that you create houses some form of personal information – be it your name, address, birthday, credit card number and verification code, or your banking information. And the gateway to that information is your password.

We don't often give passwords the credit they are due. They keep our information protected and known only to those with that confidential piece of information. Unfortunately, there are individuals who do try to hack accounts and gather our information to use it maliciously. In order to defend ourselves or our organizations from these attacks, we need to strengthen our first line of defense – our passwords. Using easy to guess passwords, like passw0rd or password123, increases your risk of hacking and having your information exposed. This can lead to devastating consequences, like identity theft or fraudulent charges on your credit card.

With every password you create, no matter how insignificant the account may seem, you should take the following steps to increase your password security:

- Password Length
  - The shorter the password, the easier to is to guess, or the quicker it takes to hack because there's fewer combinations to try. Keep passwords at least 8 characters long – this greatly increases the number of different combinations it could be, exponentially decreasing the changes that your password could be checked and increasing the time it would take to guess your password.

- Password Complexity
  - Use a combination of upper and lowercase letters, numbers, and special characters. Like password length, this will increase the number of different combinations and time taken to hack your password. According to the website Password Depot, a 9 character password consisting of 2 uppercase letters, 3 lowercase letters, 2 numbers, and 2 special characters would take over 9 years to guess.

- Password Content
  - Although it may seem easy to remember your password if it's the date of your anniversary, combination of letters and numbers chosen for your password should not be personally relevant. With the amount of information that is now available about each of us online, these relevant details are usually the first thing tried when trying to hack someone's account. Having your birthday listed on Facebook, an Instagram post for your anniversary, or pictures of your dog are all different pieces of information that hackers will access and try to use to figure out your password. Using an arbitrary string of characters makes it harder to guess and increases your password security.

If you're having difficulty remembering your passwords, a password keeper or manager may be helpful!

- ## Always Create a Novel Password
    - Having a strong password for each of your accounts is key, not just one. Anytime you update your password, it should be a new one, not one you previously used or are currently using on another account. Re-using passwords increases your risk of a security breach and gives others the opportunity to access more of your accounts.

- ## Use Two Factor Authentication When Possible
    - Lots of companies and websites allow for two factor authentication, a two-step process to signing in that is meant to increase security. Often, the two steps include inputting in your account password, which then prompts a phone call or text to be sent to a personal device with a time sensitive temporary access code to then be entered before being able to access your account. Having two factor authentication increases account security as it requires someone to have knowledge of your password and access to your device.

Next time you log in to your account, think about the password you set, and if it is maximizing your protection against security threats. The best action you can take against potential security threats is to be proactive and arm your accounts with a secure password that will keep any hackers guessing.

Kyle Hacker is the CEO of TJMicro Ltd – your complete source for professional IT services. Kyle has diverse experience in managing professional IT services and strives to meet the needs of all his clients. TJMicro Ltd provides tailored services to organizations of all sizes and across the private and public sector. To find out more about what TJMicro can do to help support your business, contact Kyle at kyle@tjmicro.com.

If you have any questions about your password security, please contact TJMicro Ltd by phone at 416-317-6000 or email at info@tjmicro.com.

To find out more about services offered by TJMicro Ltd, visit us at www.tjmicro.com.

TJ MICRO

Your complete source for professional IT services