Cybersecurity Awareness Month: Kickoff

October 2, 2023

Happy Cybersecurity Awareness Month!

McLennan Community College (MCC) is recognized as a 2023 Champion Organization with the National Cybersecurity Alliance (NCA). We believe continuous education and learning is vital to protect personal and organizational data. The ISS – Cybersecurity Team hopes to bring awareness and understanding to students, faculty and staff about the part we all play in defending against cyber threats.

MCC Campus Event: Today, Monday, October 2nd

- **Who:** Open to students, faculty, and staff
- **What:** ISS – Cybersecurity Team Event
- **When:** Today – Monday, October 2nd from: 1130am – 130pm
- **Where:** Table outside the MAC building

Have you ever heard the term “pwned” [pronounced: OHND]? No, it is not misspelled. The term was first introduced in a video game and is a take on the word “owned” – the “o” and “p” are next to each other on the keyboard. The term implies someone has been controlled or compromised.

You may be wondering; have I been pwned? Come see us today to check if your email has been compromised. We have a QR discount code, for helpful tools, password tips and fun giveaways!

2023 Key Behaviors

Enable Multi-Factor Authentication

Use Strong Passwords and a Password Manager

- Update Software
- Recognize and Report Phishing

Passwords are the keys to your digital house. Just like housekeys, you want to do everything you can to keep your passwords safe.

Multi-Factor Authentication (MFA)

This is sometimes called two-factor authentication or two-step verification. It is a cybersecurity measure for an account and requires anyone logging in to prove their identity in multiple ways. Typically, you enter your username, password, and then prove your identity some other way, such as responding to a text message.

Why go through the trouble? MFA makes it extremely hard for hackers to access your online accounts, even if they have your password. It adds another layer of security and peace of mind.

Strong Passwords

All passwords should be created with three principles in mind: long, unique, and complex. Creating, storing and remembering passwords can be a pain, but the truth is passwords are your first line of defense against cybercriminals and data breaches.

Every password should be at least 12 characters long. Each account needs its own unique password – never reuse passwords. This way, if one of your accounts is compromised, other accounts remain secure. This does not mean changing one character or adding a “2” at the end – none of your passwords should look alike. Each unique password should be a combination of upper- and lower-case letters, numbers, and special characters.

Time for Hackers to Brute Force a Password

Many times, hackers obtain passwords through a brute force attack. They use automation and scripts to try and guess passwords. This allows hackers to make a few hundred guesses every second!

Brute force attacks make it easy for cybercrimes to hack simple passwords. The more characters in a password with the addition of numbers, upper and lowercase letters, and symbols, the odds of a brute force attack decrease significantly.

As you can see, in the table below – passwords with at least 12 characters using numbers and upper and lowercase letters – the time to hack is 53 years. Adding symbols increase the time to hack to 226 years!

Number of Characters in Password	Numbers Only	Lowercase Letters	Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters	Numbers, Upper & Lowercase Letters, Symbols
4-6	**Instantly**	**Instantly**	**Instantly**	**Instantly**	**Instantly**
7	**Instantly**	Instantly	**1 sec**	**2 secs**	**4 secs**
8	Instantly	Instantly	**28 secs**	**2 mins**	**5 mins**
9	Instantly	**3 secs**	**24 mins**	**2 hours**	**6 hours**
10	Instantly	**1 min**	**21 hours**	**5 days**	**2 weeks**
11	Instantly	**32 mins**	**1 month**	**10 months**	**3 years**
12	**1 sec**	**14 hours**	**6 years**	**53 years**	**226 years**

How often do I need to change my password? If your passwords are created with these principles, you do not need to change it. You only need to change if you are aware of an unauthorized person

accessing your account, or the password was part of a data breech. If you frequently change your password, you risk reusing old passwords or creating similar/weak passwords.

Password Manager

Remembering all my passwords is so hard! This is where a password manger comes into play. This is similar to a vault with all of your passwords in one place. You only need to remember the vault combination to open and access all of your passwords. They take the form of apps or may be included automatically in your browser or operating system (OS). Apple’s iCloud Keychain is an example of a password manger.

With a few clicks, you can generate new, secure passwords that are long, unique, and complex. The password manager automatically stores passwords and can autofill them when you arrive at the applicable site. When you log into a site, your password manager will ask if you want to store the password – click yes, and another account is secured. To keep it extra safe, secure it with MFA.

Password managers are best for keeping your passwords safe. Some advantages include: saves time, works across all your devices and OS, protects your identity, notifies you of potential phishing websites, and alerts you when a password has potentially become compromised.

Is this safe? Yes. Password managers use: encryption, multi-factor authentication, and zero knowledge. Your passwords are basically impossible to decode if a hacker tried to breech your password manger. The best password managers require MFA to login. This creates extra security and requires anyone trying to view your password from an unfamiliar device to login multiple ways. A password manager does not know what your password is – the company never stores your main password on the system’s servers. You are the only one with the vault combination.

Get Social

Do you have any tips or tricks? Share and tag your posts:

- #CybersecurityAwarenessMonth
- #BeCyberSmart
- #StaySafeOnline

Revision #1
Created 6 February 2025 22:01:51 by Laura J. Crapps
Updated 6 February 2025 22:12:07 by Laura J. Crapps