ITS Communications

Algonquin College
Cybersecurity Awareness Month
2024

Password Security Best Practices

Your password is the key that unlocks your accounts. It's also one of the most valuable pieces of information an attacker can obtain. No matter your role within our College, your password can be the key an attacker is looking for, so protecting it is essential.

01 Use a Passphrase.

Use a sentence with spaces (it counts as a special character). This allows you to type naturally and avoid errors when prompted for your password. It's also easier to remember. When site policies require numbers, switch out a character for a number (i.e. r0le)

02 Make it unique.

Use one password per account login. If possible, try to also vary your username when the website or application allows. If your credentials get compromised, threat actors can spray these across other applications or websites to gain entry.

03 Enable MFA.

Adding an additional authentication factor adds another layer of security. Whenever an application or website allows you to enable multifactor authentication, enable it. Always choose an out of band option over SMS when possible. MFA will become enforced stating November 2024

04 Lock it up.

Now that you've created unique a username and password for each of your accounts, it can be daunting to manage, let alone remember. This is where using a password manager is helpful. See list of recommended password managers here

05 Never save passwords in your browser.

Saving passwords in your browser can lead to a compromise. Remember to use a password manager for both personal and work accounts. Check with your provider for a browser integration for a better experience.

Information Security & Privacy is Everybody's Business