

Cybersecurity Awareness Month
October 2026

SECURE TODAY READY TOMORROW

When it comes to safeguarding our sensitive data and records, the first and most important line of defense is a strong, unique password that's securely kept and used in combination with multifactor authentication (MFA). We've unpacked some basic do's and don'ts in the chart below so you have an easy reference guide you can use in your day-to-day activities, whether at home or at work.

DO!	DON'T!
Create complex passwords using a mix of uppercase letters, lowercase letters, numbers, and special characters	Use predictable patterns like common words, names of family members, or simple sequences like "Algonquin123"
Use at least 12 characters as longer passwords are significantly harder to crack	Reuse passwords across multiple accounts
Use generic numbers and words avoiding using personal information such as birthdays, names, addresses, or phone numbers	Store passwords insecurely in plain-text documents, sticky notes, unsecured files, default browser password vaults, etc.
Enable Multifactor Authentication wherever available for an additional layer of security	Share passwords with anyone, including family members, colleagues, or friends
Use a password manager to securely generate and store unique passwords for each account	Enter your password after clicking an unfamiliar or suspicious link

For additional information and guidance, check out this great animated video from the Canadian Centre for Cyber Security: [Creating a Strong Password](#). And lastly, here are a few important tips to keep in mind:

- **ITS will never ask for your password** over email, phone, or chat
- **Report suspicious activity to ITS immediately** including unexpected login prompts or password reset requests
- **Review your account security settings** regularly to ensure they're up to date
- **Exercise caution** when entering credentials on unfamiliar websites, verify the URL before logging in

If you're on campus in Ottawa on Monday October 19th, please join us at our awareness booth from 11AM to 2PM, outside of Salon A in D Building. We'll have trivia, activities, and chances to win some great swag! If you can't make the booth, any questions you might have about cyber security or keeping your data safe can be sent to ITS Client Care at 613-727-4723 ext. 5555 or at 5555@algonquincollege.com.