

As this year's Cybersecurity Awareness Month comes to a close, we wanted to take a moment to recap the great tips, information, and guidance we've shared with you over the last four weeks to help you stay secure. Here is a roundup of the key takeaways:

1. **Post secondary institutions are attractive targets for cyberattacks** because they store valuable and wide-ranging data including personal, research, financial, and administrative information.
2. **Be wary of cybercriminals using various types of phishing methods** to impersonate trusted individuals or organizations in an effort to trick you into revealing sensitive information, clicking malicious links, opening infected attachments, or approving unauthorized requests.
3. **If you see something, say something!** Every member of the College community shares responsibility in keeping each other and our data secure. By remaining alert to warning signs and promptly reporting suspicious events like unexpected attachments, urgent requests, unusual emails, unfamiliar devices, or abnormal network activity, you can help stop malicious actors in their tracks.
4. **Strong passwords used with multifactor authentication (MFA) remain one of the most effective defenses against unauthorized access.** You should enable MFA whenever possible, and ensure your passwords are strong, complex, use at least 12 characters, and do not contain personal details like birthdays or pet names. Consider also using a password manager to keep your login credentials secure.
5. **Cybersecurity and privacy work in tandem to safeguard our accounts and data.** Cybersecurity protects systems and data from unauthorized access, while privacy governs how personal information is collected, used, disclosed, and retained. Together, these disciplines help safeguard the wealth of information held by the College.

Overall, the newsletters we've published over the last four weeks have emphasized that awareness, strong security habits, timely reporting, responsible information handling, and shared responsibility are essential to protecting both ourselves, each other, and the College from evolving risk. Thank you for your ongoing diligence and doing your part to safeguard our College community!

As always, we're here to answer any questions you might have about cyber security and keeping your data safe. You may reach out to ITS Client Care with your questions at 613-727-4723 ext. 5555 or at 5555@algonquincollege.com.