

Cybersecurity Awareness Month
October 2026

SECURE TODAY READY TOMORROW

Welcome to week one of Cybersecurity Awareness Month! For our first newsletter, we'll explore what phishing and ransomware are, and how these kinds of attacks work.

Educational institutions like ours are increasingly targeted by scammers because we hold valuable data including student records, research, and financial information, so understanding these threats is crucial to protecting against them.

Phishing

Phishing is one of the most common cyber threats we face today and can take many forms like email, text message, or voicemail. Scammers first pretend to be a trusted source like a family member, colleague, or service provider, which AI is making increasingly easier to do. Through the use of fear, curiosity, and/or a sense of urgency, the scammer attempts to trick you into revealing sensitive information like a password or bank account number, clicking malicious links, opening infected attachments, or approving unauthorized requests.

Common signs of a phishing scam can include:

- Unexpected requests to verify your account, reset your password, or provide sensitive info
- Urgent or threatening language pressuring you to act immediately
- Unusual requests involving payments, gift cards, banking information, or confidential data
- Suspicious links or attachments that you were not expecting
- Spelling, grammar, or formatting errors that seem out of place

Ransomware

Ransomware is a type of malicious software (malware) that locks you out of your files or systems until a ransom is paid. These attacks can freeze operations, leak personal data, and severely impact our College's ability to function. Attackers often gain access through phishing attempts using infected links or attachments, by using stolen credentials from reused passwords or compromised accounts, or via unpatched software or outdated systems. Once inside, malware silently spreads across your machine and network before encrypting critical files. Once you're locked out, payment will be demanded by the attacker in order to regain access.

Common signs of a ransomware scam include:

- Emails or texts urging you to download an attachment or enable macros in a document which is a small program script that can carry malicious commands
- Suspicious links asking you to log in or "verify" your account
- Unusual pop-ups, slow system performance, or locked files

Whether you're facing phishing or ransomware scams, when in doubt:

- **Stop** before taking action.
- **Look** for warning signs.
- **Verify** the request through a trusted source.
- **Report** suspected or real threats using the red shield Report button in Outlook

If you have any questions about phishing or need help identifying suspicious emails, please reach out to ITS Client Care at 613-727-4723 ext. 5555 or at 5555@algonquincollege.com.