

Cybersecurity Awareness Month
October 2026

SECURE TODAY READY TOMORROW

For today's Cybersecurity Awareness Month newsletter, we're going to unpack identity threats, and what these hazards look like in the real world. Identity threats refer to risks where the identity of an individual or organization is compromised. While this can happen as a result of accidental human error, more often than not identity threats are due to malicious attacks.

These threats typically involve unauthorized access to sensitive information, such as login credentials, personal data, or financial details. Common tactics used by attackers to exploit weaknesses in identity management systems include:

- **Phishing** whereby a scammer impersonates someone trusted to trick you into sharing information or taking actions that expose you to risk, as discussed in our last newsletter;
- **Credential stuffing** which is an automated cyberattack where hackers use stolen username and password pairs to fraudulently gain access to user accounts which is why using weak passwords or reusing old ones creates such significant vulnerability; and
- **Synthetic identity fraud** involving the creation of a new identity using both real and fictitious information usually stolen from children, the elderly, or the deceased, allowing the attacker to carry out fraudulent activity like taking out loans or applying for credit cards.

The rise in identity threats today is due in large part to the growing sophistication of cybercriminals and the tools they use, combined with the widespread use of digital identities. These circumstances have created a broad base of targets for attackers to identify and exploit.

To protect ourselves against these growing threats, let's look at some basic cybersecurity practices we can implement in our day-to-day activities:

- **Use a secure Wi-Fi network** by changing your default network name and password to something unique and avoiding use of public Wi-Fi for sensitive activities, though if you must, use a VPN if relying on a public connection.
- **Use security tools and software** such as firewalls, anti-virus software, and anti-phishing software, and be sure to keep your software applications fully updated to stay current with patches and security upgrades.
- **Secure your accounts** with strong, unique passwords that are not duplicated across devices/applications used in combination with multi-factor authentication or passkeys.
- **Share your personal information wisely** and research who you are disclosing data to before signing up for services and accounts, including reviewing company privacy policies to find out how third parties may handle your personal information.
- **Manage and monitor your accounts** by regularly reviewing your online and financial profiles for suspicious activity, and for accounts you are no longer using be sure to remove any personal information associated with it and delete the account.

We hope the information and tips we've provided in this newsletter are helpful to you and keeping your identity secure against misuse and attack. As always, if you have any questions about cyber security or need help identifying suspicious emails, please reach out to ITS Client Care at 613-727-4723 ext. 5555 or at 5555@algonquincollege.com.