Cybersecurity Newsletter

In This Issue

Educational institutions remain one of the most targeted sectors for cyberattacks. With large user populations, sensitive student data, financial systems, and research assets, our campus requires ongoing vigilance and shared responsibility.

This month's newsletter highlights key risks and practical steps we can all take to stay secure.

Cybersecurity Issues Directly Impacting the Education Sector

Top Threat This Month: AI-Generated Phishing

Security researchers and companies like Microsoft are warning about **AI-powered phishing emails**.

Hackers now use artificial intelligence to create **very realistic messages** that look like they come from:

- Banks

- Employers
- Delivery companies
- Tech support

These emails may ask you to:

- Click a link
- Reset your password
- Confirm personal information

Red flags to watch for

- Unexpected login alerts
- Urgent requests for payment or verification
- Links that don’t match the official website

✓ **Tip:** If you're unsure, go directly to the website instead of clicking the email link.

Password Safety Reminder

Weak passwords are still one of the biggest causes of hacked accounts.

Experts recommend using a **password manager** such as:

- 1Password
- Bitwarden
- LastPass

These tools help you:

- Create strong passwords
- Store them securely
- Automatically fill them in when needed

✓ **Quick rule:**

Never reuse the same password across multiple websites.

Turn On Multi-Factor Authentication (MFA)

Multi-Factor Authentication adds an extra layer of security by requiring a **second step when logging in**.

Common apps include:

- Google Authenticator
- Microsoft Authenticator

Even if someone steals your password, they **cannot access your account without the verification code**.

Online Shopping Scams Increasing

Cybercriminals often pretend to be shipping companies like:

- FedEx
- UPS

You might receive a message saying:

"Your package delivery failed. Click here to reschedule."

These links can lead to **fake websites that steal your information**.

✓ **Tip:** Always track packages using the official website or app.

Update Your Devices

Keeping your devices updated protects you from known vulnerabilities in software like:

- Microsoft Windows
- macOS
- Android
- iOS

✓ Turn on **automatic updates** whenever possible.

Quick Security Habits

Good cybersecurity is mostly about **everyday habits**:

✓ Lock your computer when you step away

✓ Avoid public Wi-Fi for banking or sensitive work

✓ Do not download unknown attachments

✓ Verify requests for money or gift cards

✓ Back up important files regularly

Security Tip of the Month

Before entering your password on a website:

1. Check the **URL carefully**
2. Make sure the site starts with **https://**
3. Confirm the domain name is correct

Example:

Hackers often use **amaz0n.com** instead of **amazon.com**.

Remember: Most cyber attacks succeed because of **human mistakes**, not technical weaknesses. Staying alert is your best defense.

If you'd like, I can also help you create:

- **An email-friendly version for staff**
- **A one-page cybersecurity awareness bulletin**
- **A monthly cybersecurity newsletter template you can reuse**
- **A version specifically for corporate employees**.

Resources for more information on Cybersecurity

https://www.getcybersafe.gc.ca/en

https://www.bleepingcomputer.com/

https://www.orion.on.ca/blog/

Subscribe to the Newsletter

To subscribe to the Conestoga College Cybersecurity Newsletter please fill out this form.