# Cybersecurity Awareness Month 2023

Version 23

Published 9/25/2023 by Giuseppe Aloisi Last updated 2/27/2024 8:46 PM by Giuseppe Aloisi

---

With multiple holidays and special events happening throughout the year, all of us at Seneca Polytechnic are excited to bring you our annual Cybersecurity Awareness Month (CSAM) this October. This article will provide an overview of CSAM and highlight how you can participate to win a variety of exciting prizes.

**What is Cybersecurity Awareness Month?**

CSAM is an annual event held around the world every October to raise awareness for cybersecurity and protect people from the rise of cyber attacks.

**2023 Phishing Derby**

During CSAM, the IT Security and Compliance Office creates a variety of phishing simulations which are sent to your Seneca email address. Should you suspect that you have been sent one of these simulations, you can report that email using the "Report Phish" red fish button and you will be entered to win that week's prize.

**2023 Security Awareness Digital Badge**

To promote cybersecurity awareness during CSAM, the IT Security and Compliance Office introduced a Foundational Online Security Awareness digital badge that both students and staff can earn by demonstrating their ability to identify suspicious emails and security knowledge. This digital badge serves as a valuable recognition of their commitment to maintaining a secure digital environment. To earn this digital badge, participants must complete a comprehensive training module on recognizing phishing emails, covering common red flags such as unusual sender addresses, misspelled URLs, and urgent language. By successfully identifying and reporting suspicious emails, individuals not only

protect themselves but also contribute to the overall security posture of our institution. This digital badge symbolizes their dedication to cybersecurity and their role as vigilant defenders of our digital community.

Users must authenticate with Seneca credentials to access the training module. Enter your Seneca username (without @myseneca.ca) and password to enter.

**Upon completion, a quiz must be completed with a passing score of 80% to receive the digital badge.**


**Prizes**

Every CSAM, Seneca Polytechnic has a variety of prizes that can be won by completing any or all of the following monthly activities.  The more activities you complete, the more chances you have to win!

Here is a list of the prizes you can win:

General prizes: one entry per reported phishing simulation and one entry by completing the Foundational Online Security Awareness digital badge

- One of two top-notch Logitech 4K webcams
- One of two AI-powered Tiny Obsbot webcams

Bonus prize: Successfully reporting all four phishing simulations during CSAM

- One of two sleek 24-inch Dell monitors

Grand prize: Completing the Foundational Online Security Awareness digital badge and reporting all four phishing simulations during CSAM

- One of three brand-new Dell Latitude 3340 laptops with 8G RAM and 256 GB SSD

*Any prizes won must be picked up at Newnham Campus
*One prize per person, winners will be contacted by Seneca email

**Weekly Tips**

Week #1

- Pay extra attention to QR codes as they may contain malicious URLs that redirect you to a phishing page. They could also download malware to your device. Scanning an

unknown QR code is no different than clicking a random link.

- Be aware of fake job opportunities and be on alert when potential employers ask you for sensitive information (passwords, bank account information, SIN number, etc.) or ask you to process a cheque for them before employment. Always check a company's reputation first before applying.

Week #2

- Report suspicious emails in your Seneca inbox to ITS using the red fish (Report Spam/Phish) button. Timely reporting will allow ITS to respond quickly on phishing emails and protect Seneca students from phishing scams.
- Create complex and unique passwords for your accounts that are hard to guess. This prevents hackers from accessing them and potentially using one compromised password to access all your accounts. Check out https://senecapolytechnic.ca/bescure for tips.

Week 3

- Enable Multi-Factor Authentication (MFA) wherever possible to make it harder for cybercriminals to steal your information. MFA adds an extra layer of security by requiring a second verification step, such as a code from a mobile app or a text message.
- Never share passwords or MFA codes with anyone. Legitimate institutions (e.g. law enforcement, government, schools, health institutions, etc.) will never send any emails or texts, or initiate phone calls to individuals asking for such information.