Cybersecurity and Keeping Yourself Safe

Teacher(s) Names (include collaborators):

Course Name: Computer Science, Health **Time Frame (in minutes):** 90

Unit/Theme: Cybersecurity, Digital Literacy **Grade Level: 9-12**

CONTENT AND SKILLS

Learning Objectives:

- **Identify online threats**: Students will learn to recognize common online threats such as phishing scams, malware, and other cybersecurity risks.
- **Create strong passwords**: Students will develop skills in creating and managing strong, secure passwords.
- **Understand encryption and access controls**: Students will be introduced to encryption and access control measures as methods to protect digital information.
- **Implement digital protection strategies**: Students will learn to apply strategies to safeguard personal and organizational information, including the use of firewalls and antivirus software.
- **Act responsibly online**: Students will demonstrate an understanding of ethical decision-making in digital spaces, reflecting on their digital footprint.

Essential Questions:

- What are the most common online threats, and how can we protect ourselves against them?
- How can we create and manage strong passwords to enhance our digital security?
- What roles do encryption and access controls play in protecting information?
- How do firewalls and antivirus software work to keep digital resources safe?
- Why is it important to manage our digital presence responsibly?

Students I can statements . . .

- I can identify and avoid common online threats such as phishing and malware.
- I can create strong passwords and understand how to manage them securely.
- I can explain how encryption and access controls protect information.
- I can recommend actions to take before and after a digital security breach.
- I can make ethical decisions that reflect an understanding of my digital footprint.

How will you meet the needs of SWD and ELL/MLL students?

- Provide visual aids and glossaries for key terms.
- Use closed captions for video resources.
- Offer additional scaffolding through peer support and simplified language resources

Content Standards

List all standard indicators (do not need standard statement)

- .

NYS Computer Science and Digital Fluency Standards
List all standards that authentically align

- 9-12 CY.1: Determine the types of personal and organizational information and digital resources that need protection.
- 9-12.CY.5: Recommend actions for digital security breaches.
- 9-12.DL.6: Manage digital presence reflecting on the permanence of online actions.

NYS SEL BENCHMARKS
https://www.p12.nysed.gov/sss/documents/SELBenchmarks2022.pdf

- SEL.3A.4.a: Demonstrate personal responsibility in making ethical decisions.

INSTRUCTIONAL PLAN
List the steps of the lesson, including instructions for the students including how they will construct and practice content knowledge.

Add Standard Indicators next to activity that aligns and highlight them.

1. **Introduction (10 minutes):**
   - Begin with a discussion on the importance of cybersecurity. **(CY.1)**
   - Show a short video illustrating common online threats.
2. **Online Threats (20 minutes):**
   - Interactive presentation on phishing scams and malware.
   - Group activity: Identify phishing attempts in sample emails. **(CY.1)**
3. **Password Security (15 minutes):**
   - Discuss characteristics of strong passwords.**(CY.1)**
   - Hands-on activity: Students create and test passwords using a password strength tool.
4. **Encryption and Access Controls (15 minutes):**
   - Brief explanation of encryption and access controls.
   - Demonstration: How encryption works in securing emails. **(CY.5)**
5. **Protection Strategies (15 minutes):**
   - Discuss firewalls and antivirus solutions. **(CY.5)**
   - Group discussion: Develop a digital protection plan for a hypothetical company. **(DL.6)**
     - Example
6. **Digital Footprint and Ethical Decisions (15 minutes):**
   - Reflect on the consequences of online actions.
   - Role-play scenarios: Ethical decision-making in online environments.
     - Examples
7. **Closure (5 minutes):**
   - Recap key points and answer questions.

- Assign a reflection task: Write about one strategy to improve personal cybersecurity.

FUTURE READY COMPETENCIES

Check off each competency that students will interact with during this lesson.

- ☑ ~~Collaboration~~
- ☐ Communication
- ☑ ~~Critical Thinking/Problem Solving~~
- ☐ Creativity & Innovation

MATERIALS / RESOURCES

Add additional resources needed for this lesson such as instructional technology templates, images, videos, etc. ***Including Instructional Technology Tools***

- Video on online threats
- Sample phishing emails
- Password strength tool
- Demonstration software for encryption
- Access to computers or tablets for activities