Unit: Cybersecurity in the Computer Science Classroom

Lesson 1: Introduction to Cybersecurity

Objective: Introduce students to basic cybersecurity concepts, including strong passwords, social engineering, digital citizenship, and cyber hygiene.

Day 1: Basic Cyber Concepts (Strong Passwords)

Lesson Objective: Students will understand the importance of strong passwords in cybersecurity.

Bellringer: Display a list of weak passwords and ask students to identify characteristics that make them weak.

Materials:
- Projector or whiteboard
- Handout: Tips for Creating Strong Passwords (from Cyber.org)

Closing Task: Exit Ticket - Students write down three strategies for creating strong passwords.

Instructions for Teachers:
1. Begin by discussing the importance of strong passwords in protecting digital assets.
2. Present tips for creating strong passwords and discuss examples.
3. Have students create their own strong passwords using the provided guidelines.
4. Discuss strategies for managing and securely storing passwords.

Interactive Activity: Pair students up and have them create a password strength meter using simple Python code.

Resources:
- Video: "Creating Strong Passwords"
- Website: Password Strength Checker

Assessment: Quiz - Multiple choice questions on strong password creation guidelines.

Lesson 2: Cyber Threats and Impact

Objective: Help students understand different cyber threats and their global impact.

Day 2: Understanding Cyber Threats
Lesson Objective: Students will identify common cyber threats and their characteristics.

Bellringer: Show a news headline about a recent cyber attack and ask students to identify the type of threat it represents.

Materials:
- Computer with internet access
- Handout: Common Cyber Threats

Closing Task: Tweet - Students compose a tweet summarizing one cyber threat discussed in class.

Instructions for Teachers:
1. Introduce common cyber threats such as malware, phishing, and DDoS attacks.
2. Discuss the characteristics and potential impacts of each type of threat.
3. Show examples of recent cyber attacks and analyze their methods and impacts.
4. Facilitate a class discussion on strategies for mitigating cyber threats.

Interactive Activity: Cyber Threat Bingo - Students play a bingo game where they match cyber threats to their descriptions.

Resources:
- Article: "Top 10 Cyber Threats of the Decade"
- Website: Cybersecurity and Infrastructure Security Agency (CISA) - Threats & Vulnerabilities

Assessment: Short quiz - Matching descriptions to cyber threats.

Lesson 3: Incident Response and Cryptography Basics

Objective: Teach students about incident response procedures and the basics of cryptography.

Day 3: Incident Response

Lesson Objective: Students will understand the steps involved in incident response.

Bellringer: Present a scenario of a data breach and ask students to identify the first step in responding to it.

Materials:
- Whiteboard or chart paper
- Handout: Incident Response Plan Template

Closing Task: Exit Ticket - Students list three steps involved in incident response.

Instructions for Teachers:
1. Explain the importance of incident response in cybersecurity.
2. Discuss the stages of incident response: detection, analysis, containment, eradication, and recovery.
3. Present a case study of a cybersecurity incident and guide students through the response process.
4. Have students work in pairs to create an incident response plan for a hypothetical scenario.

Interactive Activity: Incident Response Role-Play - Students role-play different roles in an incident response team.

Resources:
- Video: "Introduction to Incident Response"
- Tool: Incident Response Plan Template Generator

Assessment: Group presentation - Students present their incident response plans to the class.

Lesson 4: Software Security and Networking Fundamentals

Objective: Explore software security concepts and networking fundamentals.

Day 4: Software Security

Lesson Objective: Students will identify common software vulnerabilities.

Bellringer: Display a snippet of code with a vulnerability and ask students to identify the vulnerability.

Materials:
- Projector or whiteboard
- Handout: Common Software Vulnerabilities

Closing Task: Tweet - Students compose a tweet explaining the importance of software security.

Instructions for Teachers:
1. Introduce common software vulnerabilities such as buffer overflows and SQL injection.
2. Discuss how these vulnerabilities can be exploited by attackers.
3. Show examples of real-world attacks that exploited software vulnerabilities.
4. Lead a class discussion on strategies for securing software applications.

Interactive Activity: Vulnerability Scavenger Hunt - Students search online for examples of software vulnerabilities and discuss their findings.

Resources:
- Article: "Top 25 Software Vulnerabilities"
- Website: OWASP - Open Web Application Security Project

Assessment: Short quiz - Identifying vulnerabilities in code snippets.

Lesson 5: Basic System Administration
Objective: Introduce students to system administration principles, including monitoring, access control, and firewalls.

Day 5: Introduction to System Administration

Lesson Objective: Students will understand the role of system administrators in maintaining cybersecurity.

Bellringer: Ask students to brainstorm tasks that system administrators are responsible for.

Materials:
- Computer with internet access
- Handout: Introduction to System Administration

Closing Task: Exit Ticket - Students list three responsibilities of a system administrator.

Instructions for Teachers:
1. Discuss the role of system administrators in maintaining the security and functionality of computer systems.
2. Introduce basic system administration tasks such as monitoring system performance and configuring access control.
3. Explain the importance of multi-factor authentication and the use of firewalls in network security.
4. Show examples of system administration tools and software.

Interactive Activity: System Administrator Simulation - Students role-play different system administration tasks in a simulated environment.

Resources:
- Video: "Understanding Firewalls"
- Website: Multi-Factor Authentication Explained

Assessment: Group discussion - Students discuss the importance of system administration tasks in maintaining cybersecurity.