RC CyberEdge

Day 1: Introduction to Cybersecurity

A Cyber Heroes Activity

Cyber Shield Tag: A Fun Introduction to Cybersecurity

Objective: To introduce students to basic cybersecurity concepts through an engaging, active game.
Target Audience: Elementary or Middle School students (adaptable for different age groups).
Materials:

- Cones or markers to define the playing area.
- Index cards or slips of paper (one per student) labeled ”Personal Data” (or you could use different types of data, like ”Password,” ”Address,” ”Birthday,” etc.).
- Optional: Colored vests or armbands to distinguish ”hackers.”

Preparation:

1. **Define the Playing Area:** Use cones or markers to create a rectangular playing field.
2. **Prepare ”Personal Data” Cards:** Write ”Personal Data” (or specific data types) on each index card.
3. **Select ”Hackers”:** Choose a few students to be the ”hackers” (adjust the number based on class size).

Day 1: Introduction to Cybersecurity - Lesson Component (Brief Review)

- **What is Cybersecurity?**
  - Explain that cybersecurity is about protecting computers, phones, and other devices from bad people who want to steal information or cause problems.
  - Use simple language and relatable examples.
- **Why is it Important?**
  - Discuss how we use digital devices for important things like schoolwork, talking to friends, and finding information.
  - Explain that if we don’t protect our information, bad things can happen.
- **Everyday Digital Safety:**
  - **Passwords:** Emphasize the importance of strong, unique passwords.
  - **Personal Information:** Explain why students should be careful about sharing their name, address, age, and other details online.

- **Internet Dangers:** Briefly discuss phishing, viruses, and other online threats.

Activity: Cyber Shield Tag - Game Instructions

1. **Distribute "Personal Data" Cards:** Give each student (except the hackers) a "Personal Data" card.
2. **Explain the Objective:** • Students with "Personal Data" cards must protect them from the "hackers."
   - Hackers try to "steal" the "Personal Data" by tagging students and taking their cards.
3. **Set the Rules:**
   - **No Running Out of Bounds:** Students must stay within the designated playing area.
   - **Tagging:** Hackers must gently tag students to "steal" their cards.
   - **Card Exchange:** When a student is tagged, they must give their card to the hacker.
   - **Safe Zones (Optional):** You can designate "safe zones" where students cannot be tagged.
   - **Card Recovery (Optional):** You could add a rule where students can recover their cards by tagging a hacker.
4. **Start the Game:** Signal the start of the game.
5. **Game Duration:** Play for a set time (e.g., 5-10 minutes).
6. **Debrief:** After the game, discuss the following:
   - How did it feel to protect their "Personal Data"?
   - What strategies did they use to avoid the "hackers"?
   - How does this game relate to real-life cybersecurity?
   - How can we protect our information online?
   - Was it harder to protect the data alone, or in groups?

Teacher Tips:

- **Adapt the Game:** Adjust the rules and complexity based on the students' age and abilities.
- **Emphasize Fun and Learning:** Focus on creating an enjoyable experience while reinforcing cybersecurity concepts.
- **Connect to Real-World Examples:** Relate the game to real-life scenarios and online dangers.
- **Encourage Discussion:** Facilitate a discussion after the game to reinforce learning.
- **Safety First:** Ensure the playing area is safe and students play gently.
- **Inclusivity:** Adapt the game to include students with disabilities. For instance, you could allow students with mobility issues to have a larger "safe zone" or pair them with a buddy.

Variations:

- **Team Play:** Divide students into teams and have them work together to protect their "Personal Data."
- **Data Types:** Use different types of "Personal Data" cards (e.g., "Password," "Email," "Social Media").
- **Cybersecurity Tools:** Introduce "cybersecurity tools" (e.g., "firewalls," "antivirus") that students can use to protect themselves. This could be represented by special armbands or tokens that provide temporary immunity from being tagged.
- **Information Sharing:** After students are tagged, require them to say what type of information was taken. This reinforces what types of information are important to keep safe.

By following this guide, you can create a fun and educational cybersecurity activity for your students!