Cybersecurity and Online Safety

Lesson: Cybersecurity and Online Safety
ISTE Standard: 7: Global Collaborator (7a)
Lesson: Protecting Your Digital Life: Staying Safe Online

Objective:
Students will create a digital presentation or infographic that demonstrates their understanding of online safety, including how to protect personal information, recognize phishing attempts, and practice safe online behaviors.

Materials:

- Computers or tablets with internet access
- Presentation software (e.g., Google Slides, Microsoft PowerPoint) or infographic tools (e.g., Canva, Piktochart)
- Handouts on cybersecurity and online safety guidelines
- Trusted research resources (websites like StaySafeOnline.org)
- Internet access for research
- Project rubric for assessment

Safety Precautions:

- Always use trusted websites and sources for research. Do not click on suspicious links.
- Ensure all online research follows proper digital etiquette and avoids interacting with unknown or untrustworthy websites.
- When working on shared devices, ensure personal accounts and documents are logged out after use to maintain privacy.

Procedures:

1. **Introduction** (Day 1):
    - Begin by discussing the importance of online safety and the potential dangers of phishing, weak passwords, and unsafe online behavior.
    - Introduce the concept of cybersecurity, explaining how it relates to protecting personal information and privacy online.
2. **Research Phase** (Day 1):
    - Provide students with a handout or presentation on common online safety topics (phishing, password protection, and privacy settings).
    - Students will then use the internet to gather additional information, ensuring they are using trusted sources like StaySafeOnline.org.
    - Take notes on important topics, highlighting key points such as identifying phishing emails, strong password creation, and social media privacy settings.
3. **Project Creation** (Day 2):
    - Students will use a presentation tool (Google Slides, PowerPoint) or an infographic tool (Canva, Piktochart) to create their project.
    - The project should include sections for phishing, strong passwords, and privacy settings, with visual examples (e.g., screenshots of phishing emails, weak vs. strong passwords, social media privacy settings).

    - Encourage students to include simple graphics, bullet points, and headers to make their project clear and easy to understand.
4. **Review and Edit** (Day 2):
    - After creating their project, students will review and edit their work to ensure the information is accurate and easy to follow.
    - Students can peer review each other's projects and provide constructive feedback.
5. **Presentation** (End of Day 2 or Day 3):
    - Students will present their project to the class, explaining what they learned about online safety and why it's important.
    - Each student will highlight the key points of their project and answer any questions posed by their peers or the teacher.

Note: Clean-up:

- Ensure all files are saved correctly and backed up if necessary.
- If any physical materials were printed, dispose of them responsibly by recycling.
- Log out of any accounts or online tools to protect personal privacy.
- Clean and organize any shared devices used during the project.

Additional Notes:

- **Deadline**: The project is due at the end of Day 3 (or a specific date assigned by your teacher).
- **Collaboration**: You may work in pairs or small groups, but each student is responsible for contributing equally and presenting their work individually.
- **Assessment**: The project will be assessed based on content accuracy, creativity, clarity, and presentation.