CONFIDENTIALITY: THE FIRST TENET OF CIA

Lesson Description: The purpose of this lesson is to focus on the first concept of the Cybersecurity CIA Triad - confidentiality. Students will examine what a "breach of confidentiality" is and the impact on their personal lives. In addition, Students will have an opportunity to create baseline examples of encryption using Caesar Cipher and Bacon's Cipher.

Prerequisite Knowledge: These students are expected to have basic computer knowledge, such as browsing the internet, engaging in social media, and performing fundamental tasks on a computer. Students may have prior knowledge of many of the terms (confidentiality, breach), but will use this knowledge to understand and interpret the terms through a Computer Technology lens.

Length of Completion: The length of the lesson is approximately 90 minutes

Level of Instruction: This lesson is intended for a high school English Class. These lessons are appropriate for 10th and 11th grade students with beginner and intermediate computer skills. Most students have been exposed to some computer courses that focus on software applications, but have had little exposure to coding at this point. They also bring Funds of Knowledge about computers from outside of the classroom.

Applicable Concepts: GenCyber Cybersecurity Concepts

- **Confidentiality**: Define confidentiality. Provide examples and use in personal and corporate settings.
- **Think Like an Adversary:** Students explore ways they can protect information (encrypting data)

NYS COMPUTER SCIENCE AND DIGITAL FLUENCY STANDARD

9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected.

9-12.CY.2 Describe physical, digital, and behavioral safeguards that can be employed to protect the confidentiality, integrity, and accessibility of information.

9-12.CY.4: Evaluate applications of cryptographic methods.

Resources that are Needed: The resources needed to complete the lessons are: Mentimeter (ranking statements), google classroom, google slides, ASCII Binary Character Table, Alphabet strip. The assessment tools are: Encryption exercise using Alphabet strip and ASCII Binary Character Table.

Sources:.

Berthiaume, Sarah (2022) *3 Principles of Infosec: The CIA Triad*. https://carbidesecure.com/resources/3-principles-of-infosec-the-cia-triad/

Gencyber Boot Camp presentation on Cryptography

https://www.mentimeter.com/

Accommodations Needed: Accommodations for English Language Learners and Students with Disability include:

- **Vocabulary embedded in the lesson.** Each vocabulary word is highlighted, provides a hyperlink to dictionary definition and is accompanied by visual when appropriate.
- **Scenarios:** Questions about and examples of "confidentiality" draw from students' prior knowledge and current school environment and allow for a broad range of anecdotal responses.
- **Modeling:** Each encryption example begins with a model and is scaffolded for complexity.

LEARNING OUTCOMES (CENTURY GOTHIC, 14 PT., WHITE, ITALIC)

LESSON LEARNING OUTCOMES

AFTER COMPLETING THE LESSONS, STUDENTS WILL BE ABLE TO:

1. Define and provide examples of the cybersecurity tenet Confidentiality.

2. List and defend ways to provide personal Confidentiality during online activity.

3. Explain why encryption is necessary to protect the information in cybersecurity.

4. Convert plaintext into ciphertext using Caesar Cipher and Bacon's Cipher

5. Describe the computer threats students face as well as

   corporations.

LESSON DETAILS (CENTURY GOTHIC, 14 PT. WHITE, ITALIC)

Interconnection: This lesson is the second in the series on Cybersecurity. The first lesson is a brief introduction to What is Cybersecurity? from CodeHS. This lesson includes a video and online quiz. The second lesson is on Confidentiality (the lesson explained in this document). The third lesson is on Integrity and the final lesson is completed during computer class. In the last lesson, students will develop code using Caesar Cipher.

Assessment:
The assessment activities used in the this lessons include:

- Formative - oral questions, pair-share and encryption exercises
- Summative - Written reflection

Extension Activities: As stated in the Interconnection section, this lesson is one of a series. Students will continue to build their understanding of the CIA tenets and continue their work with encryption through coding exercises.

Differentiated Learning Opportunities:
The encryption exercises are scaffolded to include one letter to multiple letter encryption. In addition, students are given choice on length and complexity when creating their own encryption.

LESSON (CENTURY GOTHIC, 14 PT. WHITE, ITALIC)

Lesson Details:

Warm Up: The lesson on Confidentiality will open with a definition of confidentiality and open ended questions on what makes something confidential and why confidentiality is important.

Lesson:

This lesson uses expository instructions. The students will receive information from the teacher via definition and model example. "I do, We do, You do" format will be used.

Link to the Google Slides:

https://docs.google.com/presentation/d/1ANEfykJ5-4pKBPK1XF0pD9Hx6nL5poJmv2Rr7X3aG7w/copy

Brief overview of the lesson flow:

Action	Activity
Opener	Define confidentiality and go over EQ
Whole group	Using Mentimeter, rank the three scenarios as high or low "breach of confidentiality." Discuss why each ranks differently.

	Case Study: Gradebook and Health information
Small Group	Pair -Share: "How to keep personal information confidential."
Whole Group	Model Encryption
Small Group/Individual	Solve encryption and create original
Individual	Reflection on confidentiality and need to protect information.