Cash Course | Grades 6+

Cybercrimes and You | Lesson Plan

What are cybercrimes and how can you protect yourself from them?

Students will develop an understanding of cybercrimes, fraud, phishing scams, and how to protect their personal information online.

Learning Objectives:

- Define cybercrimes and understand their impact.
- Promote responsible online behavior and awareness.
- Define key terms associated with cybercrimes, such as impersonation and phishing scams.
- List actions to take in order to handle cybercrimes wisely, such as staying engaged, cautious, and suspicious.

Key Vocabulary:

- **Cybercrimes:** Criminal activities carried out through electronic devices.
- **Hacking:** Using computers to gain unauthorized access to data.
- **Phishing:** Online scam that tricks people into revealing confidential information.
- **Malware:** A computer virus that spreads from one computer to another.
- **Impersonation**: Cybercriminals pretend to be someone else to access personal information.

Educational Standards: CCRA.R.7, CCRA.R.1, CCRA.W.2, CCRA.W.6, CCRA.R.7, CCRA.SL.1, CCRA.SL.2

Academic Subject Areas: Financial Literacy, Money, Life Skills

What You'll Need

- Video: *Ca$h Cour$e: Cybercrimes & You* (Watch Here)
- Worksheet: *Ca$h Cour$e: Cybercrimes & You* (Click Here)

Lesson Plan (45 mins.)

Warm-Up: (10 mins.)

1. Begin the lesson with a scenario to set the stage for learning about cybercrimes and online safety. Have them imagine waking up one day to find that their social media accounts have been hacked and embarrassing posts have been made in their names. Their personal information, including photos and messages, is now public for everyone to see. Ask students:
    - How would you feel?
    - What would you do to regain control of your online presence?

Scan to watch episode:

2. Ask students to take a moment to reflect on the scenario individually and then share their thoughts with a partner, in a small group, or with the whole class. Encourage them to discuss their feelings, concerns, and potential actions they would take in such a situation.
3. Ask the students what they already know about cybercrimes and write down any questions they want answered on the board. Share that "cyber" means computer, and “crime” means illegal activity.
4. Introduce the lesson objectives and key vocabulary. Explain that today's lesson will provide them with knowledge and strategies to protect themselves in the digital world.

Watch and Discuss: (25 mins.)

1. Show the video *Ca$h Cour$e: Cybercrimes & You* for the students.
2. Pause at opportune moments in the video to ask questions and check for understanding of key vocabulary words and their meaning.
    - What is a cybercrime?
    - How do cybercrimes affect businesses and negatively influence the economy?
    - What is identity theft?
    - What does it mean that hacking is “undetectable?”
    - Describe different types of malware (spyware, ransomware, worms, and trojans).
    - Once a cybercriminal has your data, what are some examples of crimes they can commit?
    - What can you do to avoid becoming a victim of a cybercrime?

Wrap-Up: (10 mins.)

1. Distribute the *Ca$h Cour$e: Cybercrimes & You* Worksheet. Have students complete it independently, with a partner, or with a small group. (These can be collected as a formative assessment if completed independently.)
2. Work through the questions as a class and discuss any areas where students need help or still have questions.
3. Wrap up the lesson by referring back to the questions the students had at the beginning of the lesson that you wrote on the board. Ask the following questions:
    - What new things did you learn about cybercrimes?
    - What steps can you take to avoid cybercrimes?

Don’t have time for the full lesson? Quick Activity (10-15 mins.)

- Distribute the worksheet and allow students to complete it while they follow along with the video.
- Or, have students watch the video at home and use the worksheet as a quick quiz the next day in class.