Cash Course | Grades 6+

Artificial Intelligence and Fraud | Lesson Plan

How can consumers protect themselves against AI-driven scams and fraud?

Students will learn about the different forms of AI-driven fraud, the risks involved, and effective strategies to protect their personal and financial information.

Learning Objectives:

- Identify different types of AI-driven fraud, including voice cloning, AI-enhanced phishing, and investment fraud.
- Evaluate steps to prevent falling victim to AI-driven scams and understand the importance of verifying information before taking action.

Key Vocabulary:

- **Artificial Intelligence** (AI): Technology enabling machines to perform tasks that typically require human intelligence.
- **AI Voice Cloning**: The use of AI to replicate someone's voice for fraudulent purposes.
- **Phishing**: Fraudulent attempts to obtain sensitive information by impersonating a trustworthy entity in digital communications.
- **Investment Fraud**: Scams that use false or misleading claims to convince people to invest money.
- **Verification**: The process of confirming the authenticity or accuracy of information.

Educational Standards: CCRA.R.7, CCRA.R.10, CCRA.W.2, CCRA.W.4, CCRA.W.7, CCRA.SL.1, CCRA.SL.2, CCRA.L.6

Academic Subject Areas: Financial Literacy, Money, Life Skills

What You'll Need

- Video: *Ca$h Cour$e: Artificial Intelligence and Fraud* (Watch Here)
- Worksheet: *Ca$h Cour$e: Artificial Intelligence and Fraud* (Click Here)
- AI fraud scenarios printed out for each group

Lesson Plan (45 mins.)

Warm-Up: (10 mins.)

1. Begin with a brief discussion on how technology, especially AI, has become a part of everyday life. Ask students if they have ever interacted with AI (e.g., illustration programs, voice assistants, chatbots).
2. Introduce the concept of AI-driven fraud. Ask if anyone has heard of scams that use technology to trick people, such as fake calls from "relatives" asking for money.
3. Distribute examples of different types of AI-driven fraud scenarios. Have small groups discuss what part of these scams gives them away. Some examples to consider:

Scan to watch episode:

    - AI Voice Cloning Scam: A student receives a voicemail from someone who sounds exactly like their mother, saying she has been in a car accident and needs money urgently. The voicemail instructs the student to wire $500 to a bank account to cover the hospital bills.
    - AI-Enhanced Phishing Email: A student receives an email that appears to be from their bank. The email has the bank's logo and uses professional language. It states that their account has been compromised and that they need to click a link to reset their password immediately.
    - Fake Investment Opportunity: A student sees a social media post that looks like it's from a popular celebrity promoting a new cryptocurrency investment. The post claims that anyone who invests will double their money within 24 hours. The link provided redirects to a professional-looking website where the student can enter their bank details to invest.
    - AI-Generated Fake Charity: A student receives an email from what appears to be a charity asking for donations to help victims of a recent natural disaster. The email includes heart-wrenching stories and images. The student is directed to donate through a link, but the email address is slightly different from the official charity's email.
4. Some discussion questions to consider for the scenarios:
    - What emotions do the scenarios play upon to try to get the student to take action?
    - What are some actions the student could take to verify the veracity of some of these claims?
    - What are the common red flags or warning signs in these scenarios that might indicate they are scams?
5. Transition to the video by explaining that the discussion highlights how AI-driven fraud can be difficult to detect and how easily emotions can be manipulated to push someone into making a quick decision. Introduce the video, explaining that it explores AI-driven scams in more detail and provides practical strategies to avoid them. Queue up the video for the class.

<u>Watch and Apply</u>: (25 mins.)

1. Watch *Ca$h Cour$e: Artificial Intelligence and Fraud.*
2. Distribute the "Ca$h Cour$e: Artificial Intelligence and Fraud Worksheet" for students to complete independently. Allow about 10 minutes for this task.
3. Review the worksheet answers as a class, addressing areas where students may need help or clarification.

<u>Wrap-Up</u>: (10 mins.)

1. Invite students to share insights they gained about artificial intelligence scams and fraud and how this knowledge can help them spot scams in the future.

2. Allow students to share how they answered the application question on the worksheet. How did they apply what they learned from the video?

Extension Activities:

- Scenario Creation: Have students work in small groups to create their own AI-driven fraud scenarios. Each group will develop a short script for a scam (e.g., a fake phone call, phishing email, or social media scam) and then role-play the scenario for the class.
- Research Project: Assign students to research a recent real-world case involving AI-driven fraud. They should focus on how the fraud was perpetrated, who was affected, and what the consequences were. Students can present their findings to the class in a brief presentation.
- Create a Public Awareness Campaign: Have students design a public awareness campaign to educate others about the dangers of AI-driven fraud. This could include posters, brochures, social media posts, or even a short video. Students should focus on conveying key warning signs and tips for avoiding scams.

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.