Acting out fraud

Students act out a skit to learn about different types of fraud.

Learning goals

Big idea

Fraud and identity theft hurt millions of Americans every year, so it's important to learn how to protect yourself.

Essential questions

- How can fraud and identity theft harm me?
- What can I do to protect my personal information?

Objectives

- Define common types of fraud and identity theft
- Understand why fraud and identity theft pose a financial risk

What students will do

- Act out a skit about identity hackers.
- Discuss and identify different types of fraud.

KEY INFORMATION

Building block:

- Executive function
- Financial habits and norms
- Financial knowledge and decision-making skills

Grade level: Middle school (6–8)

Age range: 11–14

Topic: Protect (Preventing fraud and identity theft)

School subject: English or language arts, Fine arts and performing arts

Teaching strategy: Cooperative learning, Simulation

Bloom's Taxonomy level: Understand, Apply, Analyze, Evaluate

Activity duration: 15–20 minutes

STANDARDS

Council for Economic Education
Standard VI. Protecting and insuring

Jump$tart Coalition
Risk management and insurance - Standard 1

Preparing for this activity

☐ Print copies of all student materials for each student, or prepare for students to access them electronically.

☐ Print copies of the "Seeing fraud in action: A script about identity hackers" script in this guide for the students.

What you'll need

THIS TEACHER GUIDE

- **Acting out fraud** (guide)
  cfpb_building_block_activities_acting-out-fraud_guide.pdf

STUDENT MATERIALS

- **Acting out fraud** (worksheet)
  cfpb_building_block_activities_acting-out-fraud_worksheet.pdf
- **"Seeing fraud in action: A script about identity hackers"** (in this guide)

Exploring key financial concepts

Millions of Americans are victims of fraud or identity theft each year. No matter where you live or how old you are, you may someday be affected by these crimes. Identity theft can happen over the phone by answering personal questions or online by clicking suspicious links or opening emails from unknown sources on your computer or phone. Companies or businesses that are genuine usually have passcodes or other methods to protect your personal information. For example, many companies now use something called two-factor authentication. This requires people to use two methods to sign into an account. Criminals can also steal your personal information from companies or businesses. Knowing how to recognize fraud and identity theft is part of becoming financially literate, because it helps you better protect yourself and your money.

TIP

Because terms and laws related to fraud and identity theft can change, students should be encouraged to always look for the most up-to-date information.

Teaching this activity

Whole-class introduction

- Ask students why it's important to understand fraud and keep their personal information confidential.
- Tell students they'll have a chance to see what fraud can look like in action by watching a skit about fraud.
- Distribute the "Acting out fraud" worksheet and the "Seeing fraud in action" script.
- Be sure students understand key vocabulary:
  - **Fraud:** An illegal act that occurs when people try to trick you out of your personal information and your money.
  - **Identity theft:** Using your personal information – such as your name, Social Security number, or credit card number – without your permission.
  - **Imposter scam:** An attempt to get you to send money by pretending to be someone you know or trust, like a sheriff; local, state, or federal government employee; a family member; or charity organization.
  - **Phishing scam:** When someone tries to get you to give them personal information, such as through an email or text message, often by impersonating a business or government agency. This can be thought of as "fishing for confidential information."
- Explain that the skit shows three types of fraud: Identity theft, an imposter scam, and a phishing scam.
- Ask for two volunteers to act out the script in front of the class.
- Assign one student the role of the hacker and the other student the role of Jayden.

TIP

Visit CFPB's financial education glossary at consumerfinance.gov/financial-education-glossary/.

Individual work

- As the volunteers act out the script, ask all the students to follow along on their copies of the script and mark up the text to identify where in the script they think fraud occurred.
  - Use whatever strategies you've taught students for marking up text. They can highlight the text, underline, or use margin notes.

- Students will review the definitions of each type of fraud and describe where in the skit each type happened.
- In the "Describing fraud" section of their worksheet, students will try to describe what each type of fraud in the script looked like in action.
- Students will then answer the reflection questions.

Wrap-up

Bring the class back together and discuss the worksheet and reflection questions.

Suggested next steps

Consider searching for other CFPB activities that address the topic of protection, including managing risk or preventing fraud and identity theft.

Measuring student learning

Students' responses on their worksheets and during the discussion can give you a sense of their understanding.

This answer guide provides possible answers for the "Acting out fraud" worksheet and for the types of fraud in the script. **Keep in mind that students' answers to the reflection questions may vary, as there may not be only one right answer.** The important thing is for students to have reasonable justification for their answers.

Answer guide

Seeing fraud in action: A script about identity hackers

Hacker: Good morning, Jayden. How are you today?

Jayden: I'm well.

[*Imposter scam*] **Hacker:** I'm calling from your cellphone company to let you know that you recently bought an app and, for some reason, the payment didn't go through.

Jayden: I don't remember buying an app.

Hacker: Oh, no problem. We can double-check that for you to make sure we have all the information that we need.

Jayden: Okay.

[*Identity theft*] **Hacker:** Now I'm going to send you an email with some information in it. Can I please go ahead and get your email address?

Jayden: Yes, it's jayden@fakeemail.com.

[*Phishing scam*] **Hacker:** Thank you! Okay. I just sent you an email with a link attached to it. All you have to do is click the link and it will reactivate your account so that you can manage your app purchases.

Jayden: Okay. I did it. Now what do I do?

[*Identity theft*] **Hacker:** Okay, I see where you clicked the link. Okay, can you give me your home address as well as the email for your parent or guardian who pays for your apps?

Jayden: My home address is 124 Main St. Centerville, KY, 01832. But I don't know my mom's email address.

Hacker: Oh, I see. Let me tell you how to get into your account to see how payment options are set up.

Jayden: Okay, got it. Oh yes, I don't see the credit card number, but I see that it says my mom's credit card is on file.

[*Identity theft*] **Hacker:** Okay. Is that a Visa ending in 4502?

Jayden: No, it's a Mastercard ending in 3256.

Hacker: Okay! I made a change so that you can make purchases now on your account.

Jayden: Okay. That sounds good.

[*Phishing*] Hacker: If you still want that app that didn't go through, it will cost $6.99. I can process that for you now. I sent a link in a text message, just click that.

Jayden: Okay, I clicked on the link. Thanks for your help!

Describing fraud

Identity theft: The hacker can steal Jayden's identity by getting and using his Social Security number, email address, and his home address.

Imposter scam: The hacker is running an imposter scam by posing as a representative from Jayden's cell service provider.

Phishing scam: The hacker obtained personal information about Jayden by sending him a link and asking Jayden to respond by clicking the link.

Seeing fraud in action: A script about identity hackers

Millions of Americans are victims of fraud or identity theft each year. No matter where you live or how old you are, you may someday be affected by these crimes. This script shows you what it can look like in action.

Hacker: Good morning, Jayden. How are you today?

Jayden: I'm well.

Hacker: I'm calling from your cellphone company to let you know that you recently bought an app and, for some reason, the payment didn't go through.

Jayden: I don't remember buying an app.

Hacker: Oh, no problem. We can double-check that for you to make sure we have all the information that we need.

Jayden: Okay.

Hacker: Now I'm going to send you an email with some information in it. Can I please get your email address?

Jayden: Yes, it's jayden@fakeemail.com.

Hacker: Thank you! Okay. I just sent you an email with a link attached to it. All you have to do is click the link and it will reactivate your account so that you can manage your app purchases.

Jayden: Okay. I did it. Now what do I do?

Hacker: Okay, I see where you clicked the link. Can you give me your home address as well as the email for your parent or guardian who pays for your apps?

Jayden: My home address is 124 Main St. Centerville, KY, 01832. But I don't know my mom's email address.

Hacker: Oh, I see. Let me tell you how to get into your account to see how payment options are set up.

Jayden: Okay, got it. Oh yes, I don't see the credit card number, but I see that it says my mom's credit card is on file.

Hacker: Okay. Is that a Visa ending in 4502?

Jayden: No, it's a Mastercard ending in 3256.

Hacker: Okay! I made a change so that you can make purchases now on your account.

Jayden: Okay. That sounds good.

Hacker: If you still want that app that didn't go through, it will cost $6.99. I can process that for you now. I sent a link in a text message, just click that.

Jayden: Okay, I clicked on the link. Thanks for your help!