



Financial Literacy Education Lesson Plan



Lesson 12: Protecting Your Financial Life

55 minutes¹

Domains

- Maintaining Financial Well-Being

Oregon High School Personal Financial Education Content Standards²

- **HS.PFE.E.2:** Analyze and apply multiple sources of information when making consumer decisions.
- **HS.PFE.E.3:** Understand and apply strategies to prevent fraud and personal identity theft.

Essential Questions

- How can I protect myself from fraud and identity theft?
- How do my everyday choices affect my risk of fraud or identity theft?

Learning Targets

I can:

- Identify different kinds of scams and fraud using real-world examples.
- Recognize potential signs of fraud or identity theft.
- Practice strategies for online safety and protection.

Supplies

1. Projector
2. Presentation slides (Note: Speaker notes are provided in the lesson plan and in the accompanying PowerPoint slides.)
3. Student handouts
4. A large writing surface such as chart paper and markers, whiteboard, or chalkboard

¹ This lesson is designed for approximately 55 minutes, but timing may vary based on student discussion, reflection, and engagement. Feel free to adjust the pacing or extend activities as needed.

² The Oregon High School Personal Financial Education Content Standards are located at:
https://www.oregon.gov/ode/students-and-family/OregonDiploma/Documents/FINAL%20PFE%20Standards_AdoptedAccessible.pdf

Preparation

1. Make copies of student handouts.
2. Set up projector with presentation slides.

Overview

This lesson helps students recognize and protect themselves from fraud. They will learn about common types of fraud and scams and how to stay safe by guarding personal information and using smart digital habits. Through discussion and examples, students will see how these tips apply to their own lives and feel empowered to safeguard their financial well-being.

Instructions

Activity 1: Warm-Up

5 minutes

1. Display the **Title slide (Slide 1)** and distribute the handout packets to students, if you have not already.
2. Display the **Warm-up slide (Slide 2)** and point students to the copy of the prompts on the slide (*What are things people do—online or offline—that help keep their money and personal information safe? Why are these important for financial well-being?*) that is provided on the first page of their handouts.
3. Invite students to take a moment to write down their responses to the prompts in the spaces provided in their handouts. Tell them there are no right or wrong answers—they should simply write whatever comes to mind.
4. Have students turn to a partner to discuss their responses together briefly.
5. After two minutes, invite a few pairs to share their best ideas with the full group.
6. Remind students of their work in previous lessons to learn and practice informed financial decision making. Explain to them that in this lesson they will learn about different types of scams and fraud and practical strategies to recognize and prevent them.
7. Display the **Learning targets slide (Slide 3)** and point students to the copy of the learning targets provided on the first page of their handouts. Review the learning targets with them.
8. Point students to the copy of the lesson glossary provided on the first page of their handouts and review the terms with them.
9. Point students to the **Note Catcher handout** and invite them to use it to take notes during the lesson.

Activity 2: Presentation

15 minutes

1. Display the **Presentation slide (Slide 4)**.
2. Display the **Scams and fraud slide (Slide 5)** and review with students the information provided. Share with students that a scam is often used to gather information or documents that are used to commit fraud. The result is often lost money and compromised accounts.
3. Display the **Youth and elders most susceptible to fraud slide (Slide 6)** and review with students the information provided.
4. Display the **Types of scams slides (Slides 7-8)**. Walk through each scam on the slides with students, inviting them to share examples of the scam they or someone they know has encountered.
5. Display the **Sample phishing scam slide (Slide 9)**, **Sample clickbait and sweetheart scam slide (Slide 10)**, and the **Sample approval scam slide (Slide 11)** to show students actual examples of clickbait, sweetheart, phishing, and fake approval scams.
6. Display the **What to do if you think your identity has been stolen slide (Slide 12)** and review with students the information provided.
7. Point students to the **Tips for Staying Safe handout** and give them a few moments to review. It provides general tips and strategies for protecting financial well-being, including instructions for responding to suspected identity theft.
8. Emphasize for students the importance of contacting a bank or credit union right away if they suspect identity theft or fraud. Financial institutions can take immediate actions to stop or limit fraud, such as cancelling debit and credit cards and recovering money from unauthorized charges. They can also offer helpful tools and advice.
9. (Optional) Provide students with a short break. The **Break slide (Slide 13)** is provided if you choose to give students a break at this point or later in the lesson.

Activity 3: Application Activity

15 minutes

1. Display the **Application Activity slide (Slide 14)**.
2. Divide the class into small groups.
3. Display the **Activity instructions slide (Slide 15)** and point students to the **Spot the Scam handout**. Review the activity instructions as a class. Students will work in groups to discuss several scenarios, decide what type of scam or fraud it represents, and describe how they can avoid falling victim to it using the spaces provided in the handout.
4. Re-display the **Types of Scams slides (Slides 7-8)** so students can refer to them as they work on the activity.
5. Invite groups to begin working.
6. Circulate among the groups as they work to answer questions and make sure they are staying on task.
7. After 15 minutes, or when it looks like the groups have completed the activity, get their attention and move on to the activity debrief.

Activity 4: Activity Debrief

15 minutes

1. Display the **Debrief slide (Slide 16)**.
2. Using the **Spot the scam answer key slides (Slides 17-20)**, have students compare their work with the answers provided on the slides.
 - If students have questions about or disagree with any of the suggested answers, encourage them to explain their reasoning.
 - Students' answers do not need to match the exact wording as long as they are conceptually or directionally correct.

Activity 5: Wrap-Up

5 minutes

1. Display the **Wrap-Up slide (Slide 21)**.
2. Display the **Exit ticket slide (Slide 22)** and point students to the copy of the prompts on the slide that is provided on the last page of their handout packets. Invite students to write their responses to the prompts in their handouts in the spaces provided.
3. Display the **Thank you! slide (Slide 23)**.
4. Answer any final questions and thank students for their participation.

Extensions

1. Have students complete the scenarios in the ***Protecting Your Financial Life Scenarios handout***.
2. Cybersecurity Awareness Month (October) is a national campaign to help people stay safe online. It started in 2004 and focuses on simple steps everyone can take, like using strong passwords, turning on multi-factor authentication, updating software, and spotting scams. Schools, businesses, and communities join in with activities and resources to build good digital habits. Following are some suggested activities to use during October (or any other month) to build students' awareness of the importance of cybersecurity.
 - The [PBS NOVA Cybersecurity Lab](#) is a free online game lets students explore real-world cybersecurity challenges through interactive simulations. Players take on roles like coding passwords, defending against phishing attacks, and securing networks while learning key concepts about online safety and data protection. Use it as a class activity or homework to spark discussion about digital security and responsible online behavior.
 - Invite students to work in groups to prepare a 20-minute presentation on digital safety for middle-school students. They can use information and materials presented in this lesson as well as online resources from OnPoint (such as "[10 Tips to Share with Your Kids About Personal Cybersecurity](#)") and the [OnPoint Guide to Personal Cybersecurity](#)) and other reputable sources.
 - Work with students to draft and sign a cybersecurity pledge. Have them agree to things like using strong passwords, enabling two-factor authentication, avoiding suspicious links, and protecting personal information. The goal is to make cybersecurity personal and encourage responsible digital behavior. See the ***Sample Cybersecurity Pledge handout*** for an example.

Glossary

Clickbait: A type of online scam that uses shocking headlines or images to trick users into clicking an unsafe link.

Fake approval scams: Scams where someone pretends a person has been approved for something—like a loan, prize, or job—that they did not apply for.

Fraud: The unauthorized use of personal information to steal money or gain access to accounts.

Identity theft: Stealing personal information to impersonate someone else, often to steal money or open accounts in the victim's name.

Multi-factor authentication: A security method that requires two or more different types of proof to confirm identity before an account can be accessed.

Passphrase: A strong, memorable password made of unrelated words, numbers and symbols.

Phishing: A scam where someone pretends to be a trusted source to steal personal information, often through fake emails or websites. Variations include *vishing* (phone calls), *smishing* (SMS/text messages), and *quishing* (QR codes leading to fake sites).

Scams: Tricks or manipulations aimed at getting people to willingly provide money or personal information.

Sweetheart scams: Scams in which scammers use emotional manipulation to gain the trust of their targets and convince them to send money or share personal information.

Too-good-to-be-true scams: Fake offers that seem amazing—like free money, a dream job, or a huge discount—but are really tricks to steal money or personal information.