



Financial Literacy Education Student Handouts



Lesson 12: Protecting Your Financial Life

Warm-Up

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?

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.

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.

Note Catcher

Main Ideas/Key Information

What are we discussing?

Notes

What did I learn?

Summary/Application

Why does it matter to me?

Tips for Staying Safe

1. Lock up important documents at home (e.g., birth certificate, Social Security card).
2. Shred old papers that contain personal information before recycling them.
3. Use strong *passphrases* with random words, numbers, and symbols. Avoid using personal info.
4. Turn on *multi-factor authentication* for important accounts (like email and banking).
5. Keep your phone, tablet, and computer locked with a password or PIN.
6. Never leave your devices unattended in public places.
7. Avoid using public Wi-Fi for banking or shopping online.
8. Check privacy settings on social media and limit what you share.
9. Be cautious of messages that ask for personal info—these could be phishing scams.
10. Review bank and credit card statements regularly for strange charges.
11. Report lost or stolen debit/credit cards right away.
12. Use trusted websites when shopping online—look for 'https' in the URL.
13. Talk to a trusted adult if something seems suspicious or you think your identity has been stolen.
14. **Contact your bank or credit union right away if you think your identity has been stolen!**
They can help with next steps such as:
 - a. Canceling compromised debit and credit cards.
 - b. Updating passwords on affected accounts and any with similar credentials.
 - c. Placing a fraud alert with a major credit bureau (Experian, TransUnion or Equifax).
 - d. Freezing your credit.
 - e. Requesting reports from creditors and debt collectors.
 - f. Filing a report with local law enforcement or at [identitytheft.gov](https://www.identitytheft.gov).
 - g. Enrolling in a credit monitoring service.

Spot the Scam

Name:

Directions:

1. Read each scenario and decide what type of scam or fraud is represented (clickbait, sweetheart scam, phishing, too-good-to-be-true, fake approval, identity theft).
2. Write down one way you could avoid the scam or fraud in the space provided. The “Tips for Staying Safe” on the previous page can provide you with some ideas.

Scenario 1: You get a text that says, “Your bank account is locked! Click this link to reset your password now.”

Type of Scam/Fraud	How to Avoid It
☐ Clickbait ☐ Sweetheart scam ☐ Phishing ☐ Too-good-to-be-true ☐ Fake approval ☐ Identity theft	

Scenario 2: Someone you met online tells you they care about you and, after a few weeks of chatting, asks you to send them money to help pay for an emergency.

Type of Scam/Fraud	How to Avoid It
☐ Clickbait ☐ Sweetheart scam ☐ Phishing ☐ Too-good-to-be-true ☐ Fake approval ☐ Identity theft	

Scenario 3: An email says you've been chosen for a \$500 gift card even though you never entered a contest. You just need to enter your full name, address, and Social Security number to claim it.

Type of Scam/Fraud	How to Avoid It
☐ Clickbait ☐ Sweetheart scam ☐ Phishing ☐ Too-good-to-be-true ☐ Fake approval ☐ Identity theft	

Scenario 4: You get a phone call from someone pretending to be a family member in trouble. They want money sent immediately through a gift card purchase.

Type of Scam/Fraud	How to Avoid It
☐ Clickbait ☐ Sweetheart scam ☐ Phishing ☐ Too-good-to-be-true ☐ Fake approval ☐ Identity theft	

Scenario 5: While scrolling online, an ad pops up offering brand new AirPods for only \$5, but you must enter your credit card information quickly before the "deal ends."

Type of Scam/Fraud	How to Avoid It
☐ Clickbait ☐ Sweetheart scam ☐ Phishing ☐ Too-good-to-be-true ☐ Fake approval ☐ Identity theft	

Scenario 6: You receive an email congratulating you on being “pre-approved” for a student loan with a super low interest rate. The email says all you need to do is provide your bank account number and Social Security number to finalize the offer.

Type of Scam/Fraud	How to Avoid It
☐ Clickbait ☐ Sweetheart scam ☐ Phishing ☐ Too-good-to-be-true ☐ Fake approval ☐ Identity theft	

Scenario 7: You notice a strange charge on your debit or credit card for a subscription you never signed up for. When you call the company, they say the account was created using your name and address.

Type of Scam/Fraud	How to Avoid It
☐ Clickbait ☐ Sweetheart scam ☐ Phishing ☐ Too-good-to-be-true ☐ Fake approval ☐ Identity theft	

Protecting Your Financial Life Scenarios

Name:

Directions:

1. Review the scenario assigned to your group (see below).
2. Answer the questions following the scenario. The “Tips for Staying Safe” section on the first page provides helpful suggestions and strategies.
3. Be ready to share your work with the whole class.

Scenario 1

Lena follows a popular influencer on Instagram who often promotes giveaways. One day, she gets a DM from an account that looks just like the influencer’s, saying she has won a \$500 gift card. The message asks her to “verify her identity” by clicking a link and entering her name, phone number, and debit card information to “cover shipping.”

- a.** What clues suggest this might not be a real giveaway?

- b.** What would you advise Lena to do?

Scenario 2

Chris gets a text that says: “Your bank account has been locked due to suspicious activity. Click here to verify your identity.” The link looks official, and Chris is worried, so he taps the link and enters his login information. A short time later, he gets a notification that someone tried to transfer money out of his account.

a. What are the red flags in the message Chris received?

b. What should Chris have done instead?

c. What can Chris do next to protect himself?

Scenario 3

Jasmine sees an ad on TikTok for trendy sneakers at 80 percent off. The website looks cool and has a countdown timer saying the deal ends in 10 minutes. She quickly enters her credit card information and places an order. A week later, the shoes did not arrive, and the website is gone. Her credit card is now showing charges from stores she has never heard of.

a. What signs suggest the site was not trustworthy?

b. What could Jasmine have done instead?

c. What should she do next to protect herself?

Scenario 4

Marcus gets a message from his best friend on Snapchat saying, “Hey, I’m locked out of my phone and need to borrow \$50. Can you send it through a cash app? I’ll pay you back tomorrow.” The profile picture and username match his friend’s, so Marcus sends the money. Later, he finds out his friend’s identity had been stolen and the message was a scam.

a. What could Marcus have done before sending the money?

b. What should Marcus do now to protect himself?

Sample Cybersecurity Pledge

I understand that cybersecurity is essential for protecting myself, my financial well-being, and the safety of others online. By signing this pledge, I agree to:

1. **Protect My Personal Information:** I will never share my passwords, personal details, or private information with anyone except trusted adults.
2. **Use Strong and Secure Passwords:** I will create strong passwords and keep them confidential.
3. **Think Before I Click:** I will avoid clicking on suspicious links, downloading unknown files, or visiting unsafe websites.
4. **Report Problems Immediately:** If I see something unusual, unsafe, or harmful online, I will report it to a trusted adult.
5. **Respect Others Online:** I will not engage in cyberbullying, hacking, or any activity that harms others.
6. **Stay Updated and Safe:** I will keep my devices updated and use security tools provided by my school.

By following these rules, I will help create a safe and responsible digital environment for everyone.

Student Name:

Date:

Exit Ticket

One scam or type of fraud I learned about today is:

A warning sign of fraud or identity theft is:

One thing I can do to stay safe online is:
