Identity Theft

Lesson 6: Teacher's Guide | Rookie: Ages 11-14

FINANCIAL FOOTBALL

Avoiding Injury with Identity Theft Protection

Identity theft protection and fraud prevention are incredibly important aspects of a healthy financial life. This 45-minute module empowers students to manage risks, monitor their financial lives, and take preventive action to protect their financial futures.

Getting Your Class Game-Ready: Training players has many benefits. It builds strength and agility, it provides time for practice and growth, and it helps minimize the risk of injury. Players work diligently to protect themselves on and off the field.

While most of us are not dodging tackles at high speeds, we do have a similar need to protect ourselves when it comes to finances. Identity theft has become increasingly prevalent and even affects children before they start building their own credit. Being aware of common risks and prevention strategies is an important step in protecting one's identity.

Module Level: Rookie, Ages 11-14

Time Outline: 45 minutes total

Subjects: Economics, Math, Finance, Consumer Sciences, Life Skills

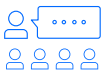
Materials: Facilitators may print and photocopy handouts and quizzes for students, or direct them to the online resources below.

- **Pre- and Post-Test questions:** Use this short grouping of questions as a quick, formative assessment with the Identity Theft module or as a Pre- and Post-Test at the beginning and completion of the entire module series.
- **Practical Money Skills Identity Theft resources:** practicalmoneyskills.com/ff43
- **Identity Theft Protection Movie Trailers (5 story lines):** Using the research tools, students brainstorm and create a movie trailer sketch to build awareness, prevent problems, and protect themselves from identity theft.
- **Two Scams and an Ad handout:** Students can play with a partner or small team to see how many identity theft risks they can identify.
- **Glossary of Terms:** Students learn basic financial concepts with this list of terms.

Icon Key

Activity

Assign the given activity to students and have them complete it individually or with a group, depending on the instructions.



Ask

Pose questions to your students and have them respond.

Assign

Designate individuals or groups to complete a particular assignment.

Debrief

Examine the activities as a whole group and compare answers and findings.

Did You Know?

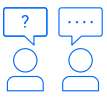
Share these fun facts with students throughout the lesson.

Pre- and Post-Test

Have students take the Pre-Test before the lesson, and take the Post-Test after completing the lesson.

Share

Read or paraphrase the lesson content to students.



Turn and Talk

Have students turn to a partner and discuss a specific topic or question.

Table of Contents

Learning Objectives

– Identify what identity theft and fraud are and how they can impact your financial life
– Examine strategies to avoid identity theft and scams
– Discover ways to handle identity theft, fraud, and/or security breaches

Key Terms and Concepts

Before you start the lesson, review the key terms and concepts below. The answers to each question will help you get students prepped and game-ready. Get deeper information around these concepts in the Facilitator Script section of this guide on pages 6 to 9 of this guide.

What is identity theft?

Identity theft can take many forms. With financial identity theft, it's often a case of bank accounts or credit cards being accessed and used illegally. For example, the thief may take out cash or max out a credit card. This can have a serious impact on your credit score. Another form of identity theft is when criminals gain access to your Social Security number and use it illegally — to take out loans or open credit card accounts, for example.

What are common types of identity theft scams?

- Phishing
- Emails
- Smishing
- Clone Phishing
- Vishing
- Skimmers
- Whaling
- Doxing

What steps can I take to protect myself from identity theft?

There are six simple steps you can take to reduce the risk of becoming a victim of identity theft or card fraud.

1. Practice safe internet use

2. Destroy unneeded financial documents

3. Guard your Social Security number

4. Check your credit report with your parents when you turn 16

5. Beware of scams

6. Secure your mail

Learning Objectives, cont.

What do I do if I think I have been a victim of identity theft?

If your private financial information gets into the wrong hands, the consequences can be devastating. If you find yourself a victim of identity theft, act quickly and contact law enforcement and the credit reporting companies.

- Report the fraud to law enforcement with your parents
- Contact the credit reporting companies with your parents
- Create a fraud recovery plan with your parents

Where can I get help and information about identity theft?

For information about fighting back against identity theft, visit the FTC's Identity Theft website (practicalmoneyskills.com/ff44) or call the hotline: 1-877-IDTHEFT (1-877-438-4338).

If you have been a victim of identity theft, immediately contact the fraud departments of each of the credit bureaus.

Did You Know?

Secure Sockets Layer (SSL) is data protocol used to keep your online transactions safe.

Credit Bureau Contact Information

Equifax
Order credit report: 1-800-685-1111
Fraud hotline: 1-888-766-0008
equifax.com

Experian
Order credit report: 1-888-397-3742
Fraud hotline: 1-888-397-3742
experian.com

TransUnion
Order credit report: 1-877-322-8228
Fraud hotline: 1-800-680-7289
transunion.com

Module Section Outline with Facilitator Script

Introduction: Warm-Up

Ask: How many of you have heard about identity theft?

Group Poll: Ask: how many children do you think have their identities stolen? (1%, 2%, 5%, 10%).

Did You Know Fact: 10% or 1 in 10 children have had their Social Security numbers used by someone else. We'll explore what identity theft can look like and ways to avoid it.

Optional Pre-Test: Have students turn to page 6 of their Student Activities guide and answer the questions with the most appropriate answer, noting a, b, c or d.

Identity Theft Basics

Share: There are many types of identity theft associated with your financial information. Here are a few common types of scams.

Did You Know?

Online phishing scams typically ask for personal information like your mother's maiden name and your date of birth.

- **Phishing** refers to scams that attempt to trick consumers into revealing their personal information such as bank account numbers, passwords, payment card numbers, or insurance account numbers.
- **Emails** that come from suspicious sources can be attempts to access your personal financial information. Do not reveal your financial account passwords, PINs, or other security-based data to third parties; genuine organizations or institutions do not need your secret data for ordinary business transactions.
- **Smishing** is similar to a phishing scam. Computer users receive an authentic-looking email that appears to be from their bank, Internet service provider (ISP), a favorite store, or other organization. Smishing messages are also sent to you via SMS (text message) on your mobile phone. Do not respond to them. Delete them and the emails.
- **Clone Phishing** is resending an email that now has a malicious attachment or link. Do not open attachments to questionable emails; they may contain viruses that will infect your computer.
- **Vishing** is where a scammer calls you pretending to be someone you know in the attempt to get your personal financial information. Potential victims may hear an automated recording informing them that their bank account has been compromised and providing a toll-free number to reenter security settings associated with the account.

Module Section Outline with Facilitator Script, cont.

- **Skimmers** are devices fraudsters install at an ATM, a gas station pump, or a store's checkout counter to copy the information from your debit or credit card.
- **Whaling** scams are directed at high-profile business individuals to get their personal financial information.
- **Doxing:** Doxing scams occur when someone releases online personal information about their victim, like their home address or cellphone number. Short for 'dropping docs,' it is a tactic hackers use to breach someone's personal data and publish it online as a means of harassment.

Preventing Fraud

Share: Being aware of common risks and prevention strategies is an important step in protecting your identity. There are six simple steps you can take to reduce the risk of becoming a victim of identity theft.

1. Practice Safe Internet Use

Delete spam emails that ask for personal information, and keep your antivirus and anti-spyware software up-to-date. Shop online only with secure web pages (check the address bar for "https" next to an image of a lock). Never email credit card numbers, Social Security numbers, or other personal information. Research mobile app privacy policies before downloading and allowing access to your social media accounts.

Did You Know?

To reduce the risk of identity theft while shopping online, only order on secure sites that begin with "https://"

2. Destroy Unneeded Personal Financial Records

Shred unneeded documents that have your personal information. These might include school paperwork with personal details, cell phone bills, ATM or debit card receipts, or statements from a checking or savings account.

3. Guard Your Social Security Number

Thieves seek your Social Security number because it can help them access your credit and open bogus accounts. Never carry your card; instead, memorize your number and store the card securely.

4. Check Your Credit Report

Credit reports show how responsibly we've used money in the past. Most youth under 18 years old will not have a credit report. However, because identity theft is rising, it's recommended to check your report around 16 years old with your parents to make sure that no one has taken your information to open fraudulent accounts. Occasionally, youth will have legitimate credit reports before 18 years old if they were added as an authorized user on a parent's credit card.

Did You Know?

One indicator of being a victim of identity theft is that your credit report shows unfamiliar activity.

5. Beware of Scams

Never give out personal information via phone or email to someone claiming to represent your bank, a

Module Section Outline with Facilitator Script, cont.

credit card company, a government agency, a charity, or other organization. If you think the request is legitimate, contact the company directly to confirm it.

6. Secure Your Mail

Empty your mailbox regularly and consider investing in a mailbox lock. When mailing bill payments and checks, consider dropping them off at the post office or in a secure mailbox.

Share: To build their agility at protecting our information, students will work in teams to create a game plan. Break students out into small groups. Each group will research and document things to watch out for (awareness), things to avoid (prevention), and things to do (protection).

Assign: Each group of students will create a one-to-two-minute movie trailer using the provided character and genre. Movie trailers must include: title, tag line, and a clear premise focused on character risks/challenges. Character risks/challenges include:

- Identity protection online (vetting websites, sharing information, etc.)
- Identity protection in real life out and about (passwords, texting, etc.)
- Identity protection at home and on your devices (privacy settings, storing personal data, etc.)

Debrief: Share group movie trailer performances and re-emphasize the importance of protecting personal information through awareness and preventive action. Add any key strategies missing in the students' movie trailers to help their characters avoid fraud and identity theft.

Putting It Into Practice

Activity: Two Scams and an Ad, played like two truths and a lie. Have students turn to page 12 of their Student Activities guide.

Two options for game-play:
Option 1: Have students play as partners or small groups to evaluate calls, emails, and marketing materials in the Two Scams and an Ad handout and determine if it is a scam or not.
Option 2: Instruct students to play by voting with their feet. Read an option aloud and have students who believe it is a scam stand and move to the right side of the room; students who do not believe it is a scam should stand and move to the left side of the room.

Getting Help If You Need It

Share: There are key things to consider when you're worried about potential identity theft, fraud, and/or security breaches. If your private financial information gets into the wrong hands, the consequences can be devastating. Let your parents know if you're receiving spam, phishing emails, or unwanted calls

Module Section Outline with Facilitator Script, cont.

or texts, or if you notice a purchase on your account that you didn't make. If you find yourself a victim of identity theft, act quickly and contact law enforcement and the credit reporting companies.

Report the fraud to law enforcement.
Report identity theft to your local police department with parental help. The police will create an "identity theft report" and you and your family can request a copy.

Contact the credit reporting companies.
Immediately contact the fraud departments of each of the credit bureaus with parental help. Alert them that you have been a victim of identity theft, and request that a fraud alert be placed in your file. You can also request a security freeze, preventing credit issuers from obtaining access to your credit files without your permission. This prevents thieves from opening new credit cards in your name.

Create a fraud recovery plan.
The Federal Trade Commission can help you and your parents create a recovery plan if you've become a victim of identity theft. When you report what happened, you'll receive a personalized recovery plan and can track your progress online step-by-step. Learn more at the Federal Trade Commission website (identitytheft.gov).

Get more information on identity theft

- Learn more about identity theft basics and ways to protect yourself at practicalmoneyskills.com/ff43
- Read the Identity Theft Practical Money Guide at practicalmoneyskills.com/ff45

Closing: Group Discussion

Ask students: what key tip would you give a friend about preventing identity theft and fraud?

Discussion

Optional Post-Test: Instruct students to turn to page 6 of their Student Activities guide to take the Post-Test.

Lesson 6 Identity Theft: Answer Keys

> Identity Theft Protection Pre- and Post-Test

> Identity Theft Protection: Movie Trailers

> Identity Theft Protection: Two Scams and an Ad

Identity Theft Protection Pre- and Post-Test

Directions: Have students turn to page 6 of their Student Activities guide and answer the questions with the most appropriate answer, noting a, b, c, d or filling in the blank.

Answer Key

1. To help prevent identity theft:

a. Keep cards and account numbers in a secure place

b. Shred documents that contain personal data

c. Never shop online

d. Both A and B

2. In which situations are you at increased risk of having your identity stolen?

a. While using an ATM

b. While shopping on an unsecured website

c. When traveling

d. All of the above

3. What information is NOT okay to share with a friend?

(Possible answers: your PIN number, your credit card account, your social media passwords)

4. A wise strategy for protecting your identity is:

a. Posting private information on social media sites

b. Giving your roommate your ATM PIN

c. Putting credit card statements in the trash

d. Using secured websites when making online purchases

5. If your wallet is lost or stolen, you should contact your debit card issuer immediately.

a. True

b. False

Identity Theft Protection: Movie Trailers

Directions: Divide students into small groups to develop a one-to-two-minute movie trailer using one of the five movie genres (mystery, action/adventure, comedy, science fiction, or superhero) and characters below. Their movie trailers should include: title, tagline, and a clear story line. Direct students to review their character's identity theft risks and challenges and understand the supporting facts before they develop their movie trailers. Instruct students to turn to pages 7 to 11 of their Student Activities guide to complete the Movie Trailers activity.

Movie Genre

Mystery

Character

Female, high school student

Character Strengths

- Creative problem solving
- Quick and skilled with technology

Character's Identity Theft Risks and Challenges

- Loves discovering and sharing new information, even if it means clicking random links
- Spends a lot of time on social media seeking out information

Supporting Facts

- It's important to be protective of private information online
- Clicking on third-party links without making sure the source is secure can open you up to malware attacks or having your personal information taken

Title:

Tagline:

Storyline:

Identity Theft Protection: Movie Trailers, cont.

Movie Genre

Action/Adventure

Character

Male, recent college graduate

Character Strengths

- Fast decision maker
- Strong communication skills

Character's Identity Theft Risks and Challenges

- Gets overexcited about opportunities to make money and is quick to share his information to land a spot
- Not sure where to look for jobs — sometimes scans local ads and social media for ideas

Supporting Facts

- Don't ever pay up front for a promise. If someone is selling a kit to start a job or requires you to pay for a training, it might be a scam
- Double-check the details — consider an online search to see if there are any past complaints

Title:

Tagline:

Storyline:

Identity Theft Protection: Movie Trailers, cont.

Movie Genre

Comedy

Character

Two best friends in middle school

Character Strengths

- Great photographers
- Quick to think up adventures together

Character's Identity Theft Risks and Challenges

- Sometimes jokes go too far and they share silly stories and other personal info on social media
- They're such close friends — why not share all their account passwords with each other?

Supporting Facts

- Convenient online sharing can come at a price: a simple overshare can lead to large privacy violations and create risk of identity theft
- Sharing passwords along with not checking privacy settings on websites and in apps can create risks for your information being taken and your activity being tracked

Title:

Tagline:

Storyline:

Identity Theft Protection: Movie Trailers, cont.

Movie Genre

Science Fiction

Character

Siblings, one older and one younger

Character Strengths

- Innovative at using technology to do amazing things
- Able to handle tough situations together and on their own

Character's Identity Theft Risks and Challenges

- Rush to try out new technology without thinking about potential risks
- Don't see tech as creating problems, just solving them

Supporting Facts

- Using new technology can present amazing new opportunities but also potential identity theft risks. It's important to consider how you store your personal data and who has access to your devices.
- Many sources suggest covering your camera, turning off GPS tracking, and regularly checking privacy settings on your devices to make sure you're preventing privacy breaches

Title:

Tagline:

Storyline:

Identity Theft Protection: Movie Trailers, cont.

Movie Genre

Superhero

Character

A middle school student who helps out at an after-school program mentoring kids

Character Strengths

- Extremely knowledgeable
- Great at research (favorite topic: scam spotting)

Character's Identity Theft Risks and Challenges

- Loves to share tips and sometimes posts the location and personal pictures of financial information as examples online
- Incredibly curious and opens all emails even if they look like spam

Supporting Facts

- The Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) both share articles, videos, and other resources to help everyone avoid scams and get help if needed.
- One of the best ways to protect yourself from identity theft is to spot and address warning signs, including: spam emails, bills for services you didn't use, and unwanted marketing phone calls asking for your information.

Title:

Tagline:

Storyline:

Identity Theft Protection: Two Scams and an Ad

Directions: Can your students spot the scam? Have them play with a partner or small team to see how many identity theft risks they can identify. Their answer should identify each scenario as a "scam" or an "ad" and explain their reason why. They should include tips or best practices for protecting their identity. Instruct students to turn to pages 12 to 13 of their Student Activities guide to complete the exercise.

Something Phishy

1. You get a call and are excited to hear you've been awarded a scholarship! They know your name, your school, and when you're graduating. They say that to finalize the award they will need your address and banking details.

   Answer: *Scam; a valid scholarship offer will not require banking info over the phone. Ask yourself: who is calling? What are they asking for and why?*

2. You get a text from a store you've only gone to once offering 50% off. The text includes a link to the national website to download the offer.

   Answer: *Most likely an ad, if this is a recognizable store and website.*

3. You get an email invite to view an online document; it's your friend's name but the email isn't one you remember your friend using.

   Answer: *Scam; avoid opening links you do not recognize. It might install malware or phish your information.*

Mal-Intent or Just Annoying Marketing?

1. You get a text with a brief survey from your favorite store two days after making a purchase there. You told the sales clerk you didn't want text offers.

   Answer: *Most likely an ad.*

2. Someone knocks on the door, selling magazines for a school fundraiser. For just $5 you can get two years of your favorite subscription. They need you to give your name, address, and credit card info. They offer a glossy handout listing the magazines but no other formal documentation.

   Answer: *Scam; avoid giving financial information to contacts you cannot validate.*

3. You get a text offering help to get scholarships; it says "Click here to sign up today for discounted access to support."

   Answer: *Scam; avoid opening links you do not recognize. It might install malware or phish your information.*

Identity Theft Protection: Two Scams and an Ad, cont.

Unexpected Sharing or Serious Issue?

1. You shared a video online explaining the solution to a math problem. The video did not show your face, just the math problem close up onscreen. Someone commented on the video, sharing your name, phone number, and email and telling others they should reach out for tutoring.

   Answer: *Scam/Identity Theft Risk: This practice of sharing personal information without the person's permission is called doxing and can cause serious problems.*

2. You download an app and it asks if it can access your personal information.

   Answer: *Most likely an ad, but it's important to protect your privacy and limit apps' access to your personal information. Consider not allowing all apps access to your camera, microphone, and GPS.*

3. Your friends shared an online quiz; it's easy to take and ends telling you which of your favorite TV characters you are most like. When you click on the link through social media, it requires access to your profile and asks permission to post your result to your profile.

   Answer: *Identity Theft Risk: While not always scams, online quizzes from random sites and apps that require access to your social media account are able to track future behaviors. Consider reading the fine print or limiting what you share with third parties.*

Glossary of Terms

Have students study this list of personal finance terms to warm up before playing Financial Football. By mastering these terms, students will have a better opportunity to answer questions in the game correctly and score.

Clone Phishing: This is resending an email that now has a malicious attachment or link. Do not open attachments to questionable emails; they may contain viruses that will infect your computer.

Credit bureau: A credit bureau is a company that gathers and stores various types of information about you and your financial accounts and history. They use this information to create your credit reports and credit scores. The three major consumer credit bureaus are Equifax®, Experian®, TransUnion®.

Doxing: These scams occur when someone releases online personal information about their victim, like their home address or cellphone number. Short for 'dropping docs,' it is a tactic hackers use to breach someone's personal data and publish it online as a means of harassment.

Identity theft: The fraudulent use of another person's information for financial gain.

Malware: Software that is intended to damage or disable computers and computer systems.

Pharming: The fraudulent practice of directing internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal financial information such as passwords, account numbers, etc.

Phishing: The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal financial information, such as passwords and credit card numbers.

Pyramid schemes: Illegal schemes in which money from new investors is used to show a false return to other investors.

Scam: A fraudulent activity or deceptive act.

Security breaches: An incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms.

Skimming: A method used by identity thieves to capture information from a card holder.

Smishing: This is similar to a phishing scam. Computer users receive an authentic-looking email that appears to be from their bank, Internet service provider (ISP), favorite store, or some other organization. Smishing messages are also sent to you via SMS (text message) on your mobile phone. Do not respond to them. Delete them and the emails.

Social Security identity theft: A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. ssa.gov/pubs/EN-05-10064.pdf

Whaling: These scams are directed at high-profile business individuals to get their personal financial information.