Identity Theft

Lesson 6: Student Activities | 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 you to manage risks, monitor your financial lives, and take preventive action to protect your financial futures.

Getting Game-Ready: Athletes who train for their sport see 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 can even affect you before you start building your own credit. Being aware of common risks and prevention strategies is an important step in protecting your identity.

Module Level: Rookie, Ages 11-14

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

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

- **Pre- and Post-Test questions:** Answer these questions before completing the Identity Theft activities to see how much you already know about the topic. After you've finished all the activities with your teacher and classmates, try taking the quiz again to see how your understanding has grown.
- **Practical Money Skills Identity Theft resources:** practicalmoneyskills.com/ff43
- **Identity Theft Game Plan activity handout:** Using the research tools, brainstorm and create a movie trailer sketch to build awareness, prevent problems, and protect yourself from identity theft.
- **Two Scams and an Ad handout:** Play with a partner or small team to see how many identity theft risks you can identify.
- **Glossary of Terms:** Learn basic financial concepts with this list of terms.

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 get you prepped and game-ready.

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:** These are scams that try to trick someone into giving away their personal information, such as bank account numbers or passwords.
- **Emails:** Beware of emails coming from suspicious sources, which may be attempts to get your personal 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:** 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), 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.
- **Clone Phishing:** This refers to re-sending an email that has a malicious attachment or link. Don't open attachments to questionable emails; they may contain viruses that will infect your computer.
- **Vishing**: Vishing is where a scammer calls pretending to be someone you know in an attempt to get your personal information. Potential victims may hear an automated recording informing them that their bank account has been compromised and providing a toll-free number to reset security settings associated with the account.
- **Skimmers:** This is when scammers install devices at an ATM, a gas station pump, or a store's checkout counter to copy the information from a shopper's debit or credit cards.
- **Whaling:** These scams are directed at high-profile business people 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.

Learning Objectives, cont.

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
5. Beware of scams
6. Secure your mail

Did You Know?

Secure Sockets Layer (SSL) is data protocol used to keep your online transactions safe. Some URLs start with "http://" while others start with "https://". Did you notice that extra "s" when you were browsing websites that require giving over sensitive information, like when you were paying bills online? The extra "s" means your connection to that website is secure and encrypted, and any data you enter is safely shared with that website.

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

Did You Know?

To reduce identity theft while shopping online, you can tell if a site is secure by looking in the address bar of your web browser. There will be a small lock icon next to the website address and the address will begin with "https://"

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.

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

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

Did You Know?

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

Student Activities

> **Pre- and Post-Test**

> Identity Theft Protection: Movie Trailers

> **Identity Theft Protection: Two Scams and an Ad**

Identity Theft Protection Pre- and Post-Test

Student Name: _____

Directions: Answer the questions with the most appropriate answer, noting a, b, c, d or filling in the blank.

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?

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: Your teacher will divide your class into small groups. Team up with your group 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. Your movie trailer should include: title, tagline, clear story line. Review your character's identity theft risks and challenges and understand the supporting facts before your team develops your movie trailer.

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 job
- 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 technology 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

Goal

- To help others learn about the risks of identity theft

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
- Is 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 you spot the scam? Play with a partner or small team to see how many identity theft risks you can identify. Your answer should identify each scenario as a "scam" or an "ad" and explain your reason. Include tips or best practices for protecting your identity.

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, which seems solid. They say that to finalize the award they will need your address and banking details.

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.

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.

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.

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

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 have a glossy handout listing the magazines but no other formal documentation.

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

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 onscreen. Someone commented on the video, sharing your name, phone number, and email, and telling others they should reach out for tutoring.

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

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.

Glossary of Terms

Study this list of personal finance terms to warm up before playing Financial Football. By mastering these terms, you 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.