Identity Theft

Lesson 6: Student Activities | Hall of Fame: Ages 18+

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 will empower you to manage risks, monitor your finances, and take preventive action to protect your financial future.

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 even affects children before they start building their own credit. Being aware of common risks and prevention strategies is an important step in protecting your identity.

Module Level: Hall of Fame, Ages 18+

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

Materials: Facilitators may print and photocopy handouts and quizzes for you, 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 list of strategies 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.

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 taking the following steps:

- Report the fraud to your bank or credit union that issued the card and request replacement cards
- Report the fraud to law enforcement
- Contact the fraud departments of each of the credit bureaus
- File a fraud report
- Create a fraud recovery plan

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

Did You Know?

You can tell if a site is secure by looking in the address bar of your web browser. When there is a small lock icon next to the website address and the address will begin with "https://" , it means your connection to that website is secure and encrypted.

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 (identitytheft.gov) or call the hotline: 1-877-IDTHEFT (1-877-438-4338).

Learning Objectives, cont.

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 that you have been a victim of identity theft is that your credit report shows unfamiliar activity.

Student Activities

> Pre- and Post-Test

> Identity Theft Protection Game Plan

> 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. Which is an effective way to prevent fraud?

a. Shredding documents that contain credit account information

b. Online shopping only on secure sites

c. Spreading purchases over various accounts

d. Both A and B

2. An indicator that you've been a victim of identity theft could be:

a. Getting a prank call

b. Your bank adding additional security measures to its site

c. Denials of credit for no apparent reason

d. You meet someone with the same name as you

3. To reduce the risk of identity theft:

a. Shred mail with personal information

b. Photocopy credit cards and keep copies in a safe place

c. Share your credit card number only when making purchases

d. All of the above

4. What are examples of safe internet use?

5. What are warning signs of scams to watch out for?

Identity Theft Protection Game Plan

Identity theft is a growing problem that causes financial damage to millions of Americans. To lower your chances of becoming a victim of identity theft, it's important to understand how to best protect your finances and personal information.

Directions: Work in teams to create a game plan for protecting yourself against fraud and identity theft. Each group will research and document things to watch out for (awareness), things to avoid (prevention), and things to do (protection) in order to stay protected. Time to get started on your game plan. Your teacher will have your group select a topic below or assign one to you.

Select Your Group's Research Focus (Check One of the Boxes Below)

☐ Protecting yourself online

☐ Protecting yourself in real life and out and about

☐ Protecting yourself at home and on your devices

☐ Protecting yourself when you travel

☐ Protecting yourself while banking

Create a Plan

Use the resources below to create a list of strategies to build awareness, prevent problems, and protect yourself.

- Identity Theft Basics: practicalmoneyskills.com/ff46
- How to Prevent Fraud: practicalmoneyskills.com/ff47
- Identity Protection While Traveling: practicalmoneyskills.com/ff48
- CFPB Fraud and Scams: consumerfinance.gov/consumer-tools/fraud/

Learning Objectives, cont.

Build Awareness

What warning signs should people watch out for when it comes to fraud or identity theft?

Prevent Possible Problems

What risks should people avoid taking with their information?

Protect Yourself

What actions can you take to protect your information?

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 risks you can identify. In your answer, identify each scenario as a "scam" or an "ad" and explain your reason. Include tips or best practices for protecting your identity against this type of fraud.

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 a cloud-based 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 the results tell 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.

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

Convenience or Con?

1. You're at a street festival with friends and decide to buy a few things at one of the booths. The person at the booth says the card scanner is in back and asks for your card, promising to be right back.

2. You're running errands with your family and someone notices the credit card reader at the gas station looks different and is sticking out slightly. Seems odd, but it still looks like the machine is working.

3. You're at the grocery store and, after you swipe your debit card, the checker offers you a game board and stickers so you can start playing the grocery sweepstakes game.

Summer Job or Position in Pyramid Scheme Scam?

1. Several friends are working as dog walkers using a new app. It lets pet owners see days you are available to work and lets you set your own rate. You mention wanting to try it and a friend sends you an invite through the app.

2. You're scrolling on a social media site when you spot a friend's meme; "Need some extra cash? Turn $5 into $40... Join my team and download the cash app below."

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

3. You see a flyer in front of a local coffee shop: "Summer job, work at home, do crafts for easy money." It includes a phone number and website info. Curious, you check out the website and see it costs $49.99 to get a starter kit of high-quality supplies.

Banking Bonus or Big Red Flag?

1. You've been traveling and get a phone call from an unrecognized number. They say they're from your bank and noticed an odd charge on your account; they need you to verify your account information before they can tell you more.

2. You're at your local bank and the teller shares that they have a special promotion going: if you open a new savings account with a minimum balance of $1,500 they will give you one of the stuffed animals on display and a $50 credit to your new account.

3. You're reading through emails and come across one from your bank; when you open it you notice the address it was sent from is slightly misspelled. It states you need to confirm your address for bank statements. Curious, you click the link and it looks like your bank website.

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®, and TransUnion®.

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.

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, if 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. Find out more at ssa.gov/pubs/EN-05-10064.pdf

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