Standard 9: **The student will identify and explain consumer fraud and identity theft.**

Beware! Identity Theft

Imagine getting a letter from the Internal Revenue Service (IRS) demanding that you pay $5,700 in back taxes.

That's what happened to Josh. He received a letter demanding he pay the government for income tax on wages he never earned.

The IRS letter said that Josh had worked at several places in five different states. But Josh is only 15 and has lived in Oklahoma all of his life. His only job was working on his grandfather's farm during the summer. He has never even visited some of the states where the letter says he worked.

What should Josh do? Should he just ignore the letter, thinking it must be for someone else? After all, he has never even had a "real" job like those listed in the letter? Funny how the government could make such a silly mistake.

Lesson Objectives

⇒ Describe the crime of identity theft.
⇒ Explain how to prevent being victimized by identity theft.
⇒ Determine what steps to take if victimized by identity theft.

Personal Financial Literacy Vocabulary

Federal Trade Commission: A federal agency that enforces consumer protection.

Fraud: Someone knowingly deceives you for his/her own personal gain.

Identity theft: Using a person's name or personal information without the person's permission for the purpose of stealing money or to get other benefits.

Introduction

Young adults are some of the most frequent targets of identity theft and other scams. Why? Perpetrators want to target people with limited experience in dealing with financial matters because they are easier to victimize. Unfortunately, no one at any age or any income level is immune from this problem.

Identity theft is one of the fastest growing crimes in the world today and can be one of the most costly problems consumers face. Consumers receive offers almost every day that sound too good to be true. Most of those offers used to come through the mail or by telephone, but today, they also come through email and the Internet. Scam artists have no national boundaries and may, in fact, be located in other countries but "doing business" in the United States.

Lesson

Identity theft means that someone uses your personal information (your name, social security number, credit card number or other similar pieces of information) without your permission. Generally, people who steal your identity use this information to rent an apartment, get a cell phone, get another credit card, or take other actions in YOUR name. Of course, they get to use whatever they have illegally purchased, and you get the bills.

According to the Federal Trade Commission, about 9 million people in the United States alone have their identities stolen each year. You may know someone who has been a victim. It can take hundreds of dollars and many hours of your time to correct the problem. Meanwhile, your credit history and your reputation suffer. You may even fail to get a job, rent an apartment, or be denied a loan or scholarship because of the negative information gathered about you, even if you had nothing to do with the

problem. Some victims have even been arrested for a crime because someone else used their names.

How Do They Do It?

ID thieves use several different approaches to get information about you. These include:

1. **Dumpster Diving.** They simply rummage through your trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit card or debit card numbers with a special device when processing your card.
3. **Phishing.** They pretend to be banks, the IRS or some other organization and send you an email or a letter (or even make a phone call) asking for personal information.
4. **Changing Your Address.** They complete a change of address card, creating a new address for you so they can receive your billing statements. Once they have the statements, they can access your account.
5. **Stealing**. They steal billfolds, purses, and even mail in your mailbox (bank statements, credit card statements, preapproved credit offers, new checks, or tax information — anything with your personal information). They may also take personnel records or bribe employees, who have access, to give them your information.
6. **Pretexting.** They use false information to get your personal information from financial institutions, telephone companies, and other sources. They pretend to be you to get the information; then they either use it against you or sell it someone else to use.
7. **Hacking.** They may hack into your computer or another computer system, including schools, credit card companies, and other places maintaining personal information.

Unfortunately, someone may use your personal information for months before you find out. Imagine the bills and fees that can accumulate against you before you know about it.

The best way to protect yourself from ID theft is to monitor your billing statements and your bank statements each month. You can also check your credit report on a regular basis to see if there is any unauthorized activity or charges on your account. By regularly checking your accounts, you can limit the damage caused by identity thieves.

As another option, you can subscribe to several business services that will monitor your monthly payments on a regular basis. Fees for these services vary greatly, so be sure that the benefits received are greater than the costs for these services before signing up. However, the final responsibility is on you!

In the box below, list some ways that someone could get personal information about you, without your permission.

1.

2.

3.

4.

5.

What did you learn from this exercise?

How to Protect Yourself from ID Theft

Unfortunately, you cannot completely protect yourself from being a victim, but there are several things you can do to minimize the potential. Following are several safety measures you may want to consider.

- Use passwords on your credit card, bank and cell phone accounts. Avoid passwords that are information others may know, such as your mother's maiden name, your birth date, your address, the last four digits of your Social Security number or your phone numbers. Also, use passwords that are a combination of letters and numbers.

- Put your personal information in a secure place, such as a small safe or lock box, to prevent others from having easy access to it.

- Only enter personal data on secure Web sites.

- Buy a small paper shredder and shred all papers with your personal information before throwing them in the trash. Be sure to shred credit card offers, credit card checks mailed from your card company, insurance forms, and other papers with your name and personal information on it.

- NEVER give out any personal information on the phone, through the mail, on the Internet, in an email, or in person unless you have initiated the contact and you are sure who you are dealing with. ID thieves can be very clever and very convincing, so avoid being tricked by their false stories. Remember, the IRS, your bank, your credit card company, and other places where you do business already have your personal information. They do not need to ask you to get it from you!

- Avoid cutting and pasting or clicking Web links from e-mails, unless you are certain it is a valid link. It may be a scam to get your information.

- Place your outgoing U.S. mail in a postal mail drop or take it to the post office instead of putting in the mailbox in front of your house, especially if mailing checks or other papers with personal information. Anyone can come by and get it. If you are leaving home overnight, have the post office hold your mail until you return.

- Leave your Social Security card in a secure place. Carrying it in your purse or billfold is not secure.

- Be careful about giving out your Social Security number or using it as an ID number. With that one number, ID thieves can find out almost everything there is to know about you.
- Carry only the identification information and the credit/debit cards that you actually need when you go out.
- Avoid responding to promotions. Identity thieves may create phony promotional offers to get your personal information.
- Keep your purse or billfold in a safe place at school and at work. Pick up orders of new checks at the bank instead of having them mailed to your home address.
- Order a copy of your credit report from the three primary credit bureaus to monitor your credit history. Because you can get a free report from each credit bureau annually, you might want to order one report from each agency about every four months instead of ordering all three at one time.

COMPLETE: Identity Theft Match – Activity 9.2.1

Ask your teacher to review your answers before continuing with this lesson.

Now that you are aware of the problem, what steps will you take to protect yourself from identity theft?

1.

2.

3.

4.

5.

Steps to Take if Victimized

If you become the victim of a fraud or even suspect you might be, let your parents know and contact your local law enforcement officials immediately. Do not be ashamed or embarrassed because you are the victim of a crime. If anyone tries to make you feel silly or guilty, walk away. You need to find someone who will help you resolve the situation, not someone who wants to blame you. Everyone makes mistakes, so it is how you deal with the mistake that makes the difference.

Your complaint is an essential resource for local, state, and federal law enforcement officials. Law enforcers review consumer complaints to spot trends and build cases against computer hackers, identity thieves, and scam artists. Several different agencies are involved in assisting fraud victims. In Oklahoma, the best place to start is by calling the Office of the Attorney General and they can direct you to right place.

The Federal Trade Commission recommends the following four actions be taken immediately if you are victimized.

1. **Contact the fraud division** of the three credit bureaus, explain that you are a victim of identity theft, and ask them to put a fraud alert on your credit files. Information for the credit bureaus is given below:

   - **Equifax** 1-800-525-6285 PO Box 105873 Atlanta, GA 30348 www.equifax.com
   - **Experian** 1-888-397-3742 PO Box 2104 Allen, TX 75013-2104 www.experian.com
   - **TransUnion** 1-800-680-7289 PO Box 390 Springfield, PA 19064 www.transunion.com

2. **Contact credit card companies** or the issuers of any other cards that were affected. Follow up all phone calls with letters and a copy of the complaint filed with the police department.

3. **File a complaint** with the Federal Trade Commission. Their Web site is www.ftc.gov and contains phone numbers, forms, and general information.

4. **Contact your local police** or the police in the city where the identity theft took place.

Conclusion

Consumer fraud has a major impact on consumers and on the overall economy of the United States. According to the FTC survey on consumer fraud in 2004, people with moderate to low incomes and lower levels of education are more likely to be victims; however, anyone can become a victim. When it comes to your money and your personal information, trust only those people you know to be trustworthy. Asking questions is not a sign of being stupid. Instead, it is a sign of being a good consumer. If you do become a victim, take immediate steps to contact law enforcement officials.

★★★★★★★★★★

To order your free annual report from one or all the national consumer reporting companies, visit www.annualcreditreport.com, call toll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You can print the form from ftc.gov/credit. Do not contact the three nationwide consumer reporting companies individually; they provide free annual credit reports only through www.annualcreditreport.com, 877-322-8228, and Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

★★★★★★★★★★

Fortunately, Josh showed the letter to his grandpa, who called the Internal Revenue Service (IRS) to get more information. He also called the Attorney General's office to find out what should be done.

They recommended Josh and grandpa contact the Social Security Administration because someone was using Josh's number. That person was getting a job, then failing to file a federal personal income tax return. That is why the IRS got involved.

It took many phone calls and letters, but eventually they got the problem resolved, and Josh's name was cleared.

Things could have been much worse for Josh if he had just ignored the letter.

Name: _____ Class Period: _____

Beware! Identity Theft
Review Lesson 9.2

Answer the following questions and give the completed lesson to your teacher to review.

1. What is identity theft?

2. Explain three methods used to steal your identity.

3. List five different steps you should take to protect your identity.

4. What should you do if you become a victim of identity theft?

Name: _____ Class Period: _____

Identity Theft Match – Activity 9.2.1

Match the following terms to the scenarios. Place the letter of the correct term in the blank in front of the scenario.

A. Changing your address

B. Stealing

C. Phishing

D. Dumpster Diving

E. Skimming

F. Hacking

G. Pretexting

___1. John throws all of the copies of his bills and credit card statements in the trash. He receives a call from his credit card company asking him if he has been to Cancun recently and purchased a large amount of diving equipment. John has never traveled outside of the United States. Which term describes how a thief got John's credit card information?

___2. Alexis has not received a bill from her credit card company for three months. She has been charging items to her credit card and has been wondering why she has not been billed. She called the company and was told that the bills had been sent to her and that she is now in jeopardy of losing her card because her account is three months overdue. Which term describes why Alexis did not receive her bill?

___3. Kaden received an email asking him to confirm his credit card information and then he clicked on the link in the email that directed him to a site that asked him to fill in the blanks with his name, social security card number and his credit card number. The site looked like the legitimate organization's site so he complied with the request. Soon after he supplied the information, he received a bill from his credit card company with several purchases he had not made. Which term describes what happened to Kaden?

___4. Jeremy ordered new checks. After several weeks he called his bank to ask why he had not received them. The bank clerk told him that the checks had been mailed a week and a half ago. When he received his bank statement, he finds that someone has been writing checks on his account. What term describes what happened to Jeremy?

___5. Mary's grandmother paid for their lunch with a credit card. The waitperson brought her back the card and she signed the receipt. A month later, several charges appeared on her grandmother's credit card bill that she had not made. What term describes what the waitperson did?

___6. Sara wants a new outfit but does not have the money to buy it. She calls her friend's credit card institution pretending to be the friend and tells the company that she has lost her credit card and needs a new one. What term describes what Sara did?

___7. Kurt is a computer nerd with exceptional skills. He is able to access computers that belong to other people. He obtains Mr. Ling's bank and credit card account numbers and uses them to order items from Amazon.com. What term describes what Kurt is doing?

Which of the people above are victims and which may be prosecuted for illegal activity? Explain your answer.