OKLAHOMA STATE DEPARTMENT OF EDUCATION
CHAMPION EXCELLENCE

Beware! Identity Theft

Standard 9

The student will identity and explain consumer fraud and identity theft.

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

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? How could the government make such a big mistake?

Lesson

As a young adult, you are one of the most frequent targets of identity theft and other scams because scammers assume you have limited experience dealing with financial matters. However, anyone – any age, any income, or any educational background – is a potential victim.

Identity theft is one of the fastest growing crimes in the world today and can be one of the most costly problems to resolve. At some point, you will probably start receiving all kinds of offers through the mail, through email, through text messages, and through phone calls because scam artists are everywhere. Unfortunately, it is not just strangers that steal your identity. Approximately 10 percent of all ID theft incidents involve a family member, and sometimes it goes undetected for many years when it happens to a child. Now called "family fraud," this kind of ID theft creates a more complicated situation to resolve because it may mean prosecuting a member of your family or paying off the debt to restore your credit score.

Approximately 15 million United States residents have their identities stolen each year with financial losses totaling more than $50 billion. It can take thousands of dollars and many hours of your time to correct the problem. You may know someone who has been a victim.

Identity theft is a special type of fraud that involves stealing your personal information (your name, Social Security number, etc.) and using it without your permission to borrow money, get credit cards, rent a place to live, get a cell phone number, or even steal your income tax refund from the Internal Revenue Service. Basically, the thieves get the products and you get the bills.

Meanwhile, your credit history and your reputation suffer. You may even fail to get a job 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. You might even be arrested for a crime you did not commit because someone else is using your name and other information.

How Do They Do It?

ID thieves use several different tactics to get information about you, such as:

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 attached to the machine where slide your card. Most skimmers are placed on ATMs or in gas stations pumps, especially in locations that are not visible to others or monitored by a camera.

3. Phishing. They pretend to be you bank, the IRS, or some other organization and send you an email, a text, or a letter (or even call you on the phone) 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 from 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 that maintain your personal information. (Note: Also beware of someone hacking into your computer or sending a pop-up warning you about viruses on your system; chances are they are scamming you).

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 credit card 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.

You can also 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. Whether you choose to monitor

your own credit reports or pay for a specialized service to do it for you, the final responsibility for protecting your identity is you.

How to Protect Yourself from ID Theft

Unfortunately, it is almost impossible to completely protect yourself from being a victim, but there are several things you can do to minimize your potential losses. Following are several safety measures you may want to consider:

- Use passwords on your credit card, bank and cell phone accounts. Avoid passwords including 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 number. Also, use passwords that are a combination of letters and numbers. It is also advisable to have multiple passwords, rather than using the same password on all of your accounts.

- 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. A secure site will either have a lock symbol or some indication that it is safe to use.

- Buy a small paper shredder and shred everything with your personal information before throwing it in the trash. Be sure to shred credit card offers, credit card checks mailed from your card company, insurance forms, and other papers that show your name, account numbers, or other personal information on them. (Note: A cross-cut paper shredder provides more security than one that just cuts paper into strips.)

- NEVER give out any personal information over the phone, through the mail, on a web site, in an email, or in person unless you have initiated the contact and you are sure who it really is. 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 for it.

- Avoid cutting and pasting or clicking Web links from texts or emails, unless you are certain it is a valid link. It may be a scam to get your information. The link sent to you may take you to a fake, look alike Web site for your bank or credit card instead of the company's official site.

- Place your outgoing U.S. mail in a postal mail drop or take it to the post office instead of putting it in the mailbox in front of your house, especially if mailing checks or other papers with personal information. Anyone can come by and take 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.

REMINDER

The best way to protect yourself from ID theft is to monitor your credit card statements and your bank statements each month.

- 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.

- Never post personal information, such as your phone number, your account numbers, or your Social Security number, on a social Web site thinking only your friends will see. You never know who might see it and use it to steal your information.

- Avoid entering personal information online or accessing bank accounts when using unsecure Wi-Fi connections at coffee shops, schools, libraries, or any other public places.

- 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.

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 from them. You need to find someone who will help you resolve the situation, not someone who wants to blame you. Everyone makes mistakes; 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 enforcement officers 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.

Oklahoma Attorney General's Office
Web: ok.gov/oag
Phone: 405-521-3921

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

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 consumer reporting companies directly for your free report.

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. It is highly recommended that you make a copy of the front and back of your credit cards, and store the information in a safe place (such as a home safe or bank safe deposit box) in case you need to contact the card issuers.

3. File a complaint with the Federal Trade Commission at www.ftc.gov. The Web site also contains phone numbers, forms, and other helpful information.

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

Conclusion

Identity theft is a significant problem for all consumers and can have a negative impact on your personal life as well as your personal finances. Identity thieves today are always looking for new and creative ways to gain access to your information for their personal gain. While teens tend to be especially vulnerable to their schemes, anyone can become a victim. When it comes to your money and your personal information, be very stingy about sharing your personal information. If you do become a victim, take immediate steps to contact law enforcement officials.

FINAL NOTE: 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. After several phone calls and letters, they eventually got the problem resolved and Josh's name was cleared. Things could have been much worse for Josh if he had ignored the letter.

This lesson was written and created by
Oklahoma educators in partnership with

Oklahoma CEE
Council on Economic Education

Name: _____ Class Period: _____

Beware! Identity Theft Review 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 scammers use 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

Match the following terms to the scenarios. Place the letter of the correct term in the blank in front of the scenario. Give the complete assignment to your teacher to review.

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? Explain your answers.

Which of the people above may be prosecuted for illegal activity? Explain your answers.