



IDENTITY THEFT

GRADE LEVEL 10-12



"TAKE CHARGE OF YOUR FINANCES"

Materials provided by: Karen Dawson, Family and Consumer Sciences Educator, Skyview High School,
Billings, Montana

Time to complete: 75 minutes

NATIONAL CONTENT STANDARDS

Family and Consumer Science Standards: 2.3.2, 2.3.3, 2.4.1, 3.2.5, 3.2.7

National Council on Economic Education Teaching Standards:

National Standards for Business Education

- Career Development:
- Economics:
- Personal Finance: VI.3-4

OBJECTIVES

Upon completion of this lesson, participants will be able to:

- Recognize ways in which identity theft occurs.
- Examine costs to the consumer when identity theft occurs.
- Produce a document that lists what the consumer can do to prevent identity theft.
- Summarize what identity thieves can do with an individual's information.
- Formulate plans for minimizing the risk of loss in the event of an identity theft.
- Select preventive measures and practices for safe on-line shopping.

INTRODUCTION

In January 2009, the Federal Trade Commission reported that 313,982 "identity theft" complaints were filed. Identity theft complaints accounted for 26% of consumer fraud complaints in 2008, making it number one on the government's list of complaints. Fraud associated with third party and creditor debt collection was a distant second with only 9% of the complaints. Approximately 7% of the victims of identity theft in 2008 were under 20 years of age.

Identity Theft:

Identity theft occurs when someone wrongfully acquires and uses a consumer's personal identification, credit, or account information. Individuals whose identities have been stolen can spend months or even years and thousands of dollars cleaning up the mess thieves have made of their name and credit record.

During a person's lifetime, there will be countless times when personal information is used during everyday transactions. This might include writing a check at the local store, charging airline tickets, renting a car, applying for a credit card, mailing in tax returns, or using a cell phone to order pizza. These transactions are the activities upon which identity thieves thrive. Each one of these transactions requires a person to share personal information, thereby increasing the possibility of someone stealing this information to commit identity fraud. An identity theft can wreak havoc on an individual's credit report, cause a person to be arrested for crimes they did not commit, or open accounts using a person's name without the victim ever realizing their personal information had been stolen.

Identity thieves obtain personal information through a variety of methods. The most common way is by stealing a person's wallet or purse. Thieves may steal mail or complete a change of address form to receive an individual's bills and statements. They may also fraudulently obtain an individual's credit report. Personal information can be found in a victim's home or on the internet. Information carelessly discarded into the trash can be stolen when a thief goes "dumpster diving." Individuals can be scammed by phone, internet, or e-mail. Finally, a thief with "insider access" to records at the workplace can learn an individual's home address, social security number, and possibly even bank account numbers if pay is directly deposited.

Once an identity thief has an individual's information, it can be used in numerous ways. Identity thieves can:

- Apply for new driver's licenses;
- Open new bank and credit accounts;
- Apply for credit cards or store credit accounts;
- Obtain cash with bank cards;
- Get jobs;
- Rent an apartment;
- Make retail purchases;
- Get a phone or other utilities;
- File bankruptcy;
- Counterfeit checks;
- Give another person's name during an arrest.

The following describes the wealth of information which can be used by identity thieves, how theft occurs, and what an individual can do to minimize risk.

Identification	How Theft Occurs	Prevention
Credit Reports	A thief may use an individual's credit report to learn all of the accounts a person has, his/her social security number, and personal information about where a person works, lives, and their bank accounts.	<ul style="list-style-type: none"> ▪ Check credit reports once per year and immediately dispute any wrong information from each of the three reporting agencies. ▪ Do not leave reports lying around. Store them in a locked file or shred.
Mail	Identity thieves may steal an individual's mail to learn his/her account numbers and personal information.	<ul style="list-style-type: none"> ▪ Deposit outgoing mail in post office collection boxes rather than unsecured mail boxes. ▪ Promptly remove mail from the mailbox. If going on vacation, request a vacation hold.
Wallets and Pocketbooks	Identity thieves may steal a wallet or pocketbook to have a wealth of personal and account information.	<ul style="list-style-type: none"> ▪ Do not leave it in plain site. ▪ Do not hang it from a chair at a public place. ▪ Use purses which close securely. ▪ Only carry what is absolutely needed. Do not carry social security cards, passports, or birth certificates unless absolutely necessary.
Bills	A thief may steal a person's bills containing his/her name, address, telephone number, bank accounts, credit, debit account numbers, and even a person's social security number. This information may be used to take over current accounts or open new ones.	<ul style="list-style-type: none"> ▪ Do not leave statements lying around. Store them in a locked file and shred information not needed. ▪ Pay attention to the billing cycle. Follow up with creditors if bills do not arrive on time.

Calling Cards	If a thief has an individual's calling card and personal identification number (if required), a person may make long distance calls to anywhere.	<ul style="list-style-type: none"> Use only calling cards which require personal identification numbers. When at a pay phone, block the number while dialing so no one can see.
Passwords	With computer passwords, a thief can easily access accounts, send messages, and/or viruses, purchase or sell items, or access online bank accounts.	<ul style="list-style-type: none"> Do not give passwords to anyone. Do not write passwords down where others may find them. Create unique passwords which include a combination of numbers and letters in large and small caps. Avoid using information such as mother's maiden name, date of birth, or social security number.
ATM, Credit, and Debit Cards	<p>If an identity thief has both an individual's automatic teller machine (ATM) card and personal identification number (PIN) money can be withdrawn from the individual's account.</p> <p>Because most stores do not ask to compare identification with the signature on the back of the card, they are easy to use in the stores, on the internet, or over the phone. This is because merchandise may be mailed to a different address than the card's bill is sent.</p>	<ul style="list-style-type: none"> Do not leave cards lying around the home or office. Carry only those which will be used. Close unused accounts and cut up the card. Use debit cards which require a PIN number. Memorize the PIN number. Do not write it down in the same place the ATM or debit card is kept. Carry cards in a separate holder from the wallet. Sign the back credit and debit cards stating "Please see I.D." Do not give out the account number unless making a purchase. Keep track of all receipts and destroy papers with the card numbers on them. Do not throw papers in the trash. Check statements for unauthorized charges.
Work Records	A thief may fraudulently obtain work records containing a person's name, address, social security number, and bank information if pay is directly deposited.	<ul style="list-style-type: none"> Make sure personal records at work are locked securely with limited access by employees.
Pre-Approved Credit Cards	Identity thieves can apply for credit card accounts using pre-approved offers and change the address so the card will be sent to them.	<ul style="list-style-type: none"> Shred any credit card offers received and not used. Cut up any pre-approved credit cards not used. If a person would not like to receive credit card offers, he/she can call 1-888-567-8688 to get off the marketing list.
Bank Account Information	With a bank account and routing number, an identity thief may be able to create fake checks and withdraw money. A thief may also access savings accounts to withdraw money.	<ul style="list-style-type: none"> Do not leave statements lying around. Store them in a locked file and shred information not needed. Use passwords. Do not have check orders mailed home. Pick them up at the bank.

Social Security Number	An individual's social security number is the key to their identity. It can be used to open new accounts, apply for jobs, obtain a driver's license, file bankruptcy, etc.	<ul style="list-style-type: none"> ▪ Do not give out a social security number unless it is used for a legitimate purpose. ▪ Ask for an alternate number on driver's licenses, insurance cards, and other materials. ▪ Do not carry social security cards in wallet or pocketbook unless necessary.
------------------------	--	---

Online Shopping:

The United States Department of Commerce reports consumers spent 26 billion dollars online in 2002. This dramatic increase in shopping online is because the internet has opened a new world of products and services for consumers. The internet contains a wealth of information. Consumers can order products from around the world. They can easily research items and compare prices with the click of a button. The internet provides an element of convenience for consumers shopping in the comfort of their own home any time of the day. However, this increase in convenience also burdens consumers with new risks. Consumers must provide personal information such as financial records, social security numbers, credit card numbers, addresses, and passwords to shop online. As a result, consumers need to become aware of the risk so they may take preventative measures to protect their personal information.

There are several tips for shopping safely online:

1. *Know the real deal* – Consumers must get all of the details before purchasing. This includes a complete description of the item, total price, delivery time, warranty information, return policies, and what to do in case of problems.
2. *Look for clues about security* – To ensure the browser is secured, it should read “shttp” or “https.” A consumer should look for these clues before entering any personal information.
3. *Use a credit card* – A credit card is the safest way to purchase items because the consumer has the legal right to dispute charges for goods and services.
4. *Use an escrow service* – If working with a company which cannot accept credit cards, an escrow service is the second safest way. An escrow service will hold a person's money until confirmation of the products or services has been received.
5. *Keep proof handy* – Print and file information about the purchase in case it is needed later.
6. *Ask about “substitute” or “single use” credit card numbers* – This new technology allows consumers to make purchases without putting his/her real account number online.
7. *Get the scoop on the seller* – Check complaint records at the state or local consumer protection agency and Better Business Bureau. Get the physical address and phone number to contact the seller offline.

What to Do if Identity Theft Happens:

Identity theft can happen no matter how careful a person may be. If a person believes he/she may be a victim, they must follow these basic rules:

1. Act immediately.
2. Keep a detailed record of correspondence and phone records including the date, contact person, and any specific comments made or actions which will occur.
3. Contact the three major credit bureaus and request a “fraud alert” on file. Follow up with a letter and copies of any documentation sent certified mail. In addition, request a credit report from each bureau and carefully check to ensure they are accurate.
4. Close all accounts which have been opened fraudulently or tampered with. When opening new accounts, use different passwords and PIN numbers.
5. File a police report with the local police or in the local community where the theft took place.
6. File a complaint with the Federal Trade Commission.

The three credit reporting bureaus are Equifax – www.equifax.com, TransUnion – www.transunion.com, and Experian – www.experian.com.

Personal Liability:

Credit Cards – The Truth in Lending Act limits a person's liability for unauthorized credit card charges to \$50.00 per card. To take advantage of this law, a person must write a letter within 60 days of the first bill containing the error. If an individual's card has been stolen, it should be reported and canceled immediately.

ATM & Debit Cards, Electronic Funds Transfers – The Electronic Funds Transfer Act provides protection. The amount a person is liable for depends upon how quickly he/she reports the loss. If a person reports a lost or stolen card within two days, they are liable for a maximum of \$50.00. Within 60 days, a person is liable for up to \$500.00. After 60 days, a person may be liable for all of the money. A person should always telephone the financial institution then follow up in writing to report any losses.

Checks – Stop payment immediately and ask the financial institution to notify the check verification service. Most states hold the financial institution responsible for losses of a forged check if the person notifies the bank within a reasonable time.

In this lesson, participants will learn about different types of personal identification information, how thieves use this information, what a person can do to protect him/herself, and what to do if they are a victim of identity theft. Participants will interview a person to determine their identity protection knowledge. In addition, they will write a short essay about what they learned.

BODY

1. Ask the participants to look through their wallets or purses and find all of the information which tells something about who they are (their identity).
 - a. Wallets and purses are the most common item an identity thief steals.
 - b. On the overhead, compile a list of information categories the participants found in their wallets. Examples: Name, address, phone numbers, credit card numbers, credit card receipts, driver's license number, insurance card, social security number, paycheck stubs, and banking information (checking and/or savings account numbers, ATM card, debit card, deposit slips)
2. Discuss ways they think this information can be used fraudulently.
3. Explain to participants they will be learning about identity protection including:
 - a. What it is;
 - b. What personal identification information thieves steal;
 - c. How the information can be used;
 - d. Ways to prevent identity theft from occurring;
 - e. What to do if they are a victim.
4. Give the *Identity Theft* PowerPoint presentation 1.3.1.G1 to explain the information necessary to understanding identity protection.
 - a. Hand out the *Protecting Your Identity Worksheet* 1.3.1.A1.
 - b. Slides 1 – 4: Identity theft
 - c. Slides 5 – 6: Information
 - d. Slides 7 – 21: How identity theft occurs
 - e. Slides 22 – 26: Shopping online
 - f. Slides 27 – 31: What to do if identity theft occurs
 - g. Slide 32: Conclusion

CONCLUSION

1. Stress the importance of protecting personal information from loss or theft.
2. Discuss with participants the types of personal identification information and what they can do.
 - a. Have each participant provide one example of a way they could protect themselves against identity theft.

Or

3. Divide participants into small groups. Hand out one *Identity Theft Scenario* question card 1.3.1.H1 to each group and have them determine what they would do for the situation. Ask each group to share their response with the rest of the class. The answers are on the *Identity Theft* answer key 1.3.1.C1.

ASSESSMENT

Hand out the *Identity Theft Interview Questions* 1.3.1.A2 and *Identity Theft Interview Essay Rubric* 1.3.1.B1. Have participants interview an individual to determine their identity protection knowledge. Participants should then write a one page essay about the identity protection knowledge of the individual they interviewed based upon the requirements on the *Identity Theft Interview Essay Rubric* 1.3.1.B1.

Or

Hand out one *Identity Theft Brochure Rubric* 1.3.1.B2 to each participant. Have participants answer the questions provided in the form of a brochure to educate others. Brochures may be multiplied and distributed among community members to help educate those not in the classroom.

MATERIALS

Protecting Your Identity Worksheet – 1.3.1.A1
Identity Theft Interview Questions – 1.3.1.A2
Identity Theft Interview Essay Rubric – 1.3.1.B1
Identity Theft Brochure Rubric – 1.3.1.B2
Identity Theft information sheet – 1.3.1.F1
Identity Theft PowerPoint presentation – 1.3.1.G1
Identity Theft Scenario cards – 1.3.1.H1

ADDITIONAL RESOURCES

www.consumer.gov/idtheft

- This federal agency Web site provides consumer information and publications.

www.consumeraction.gov

- This service is provided by the Federal Citizen Information Center of the U.S. General Services Administration.

www.pueblo.gsa.gov

- The Consumer's Resource Handbook available on this government Web site lists local, state, and federal agencies, major trade associations, and consumer groups.

PROTECTING YOUR IDENTITY WORKSHEET

	Total Points Earned
47	Total Points Possible
	Percentage

Name _____

Date _____

Class _____

Directions: Complete the following questions.

1. What is the definition of identity theft? (1 point)
2. What are three examples of personal identification? (3 points)
3. What are three ways personal identification information can be used fraudulently? (3 points)
4. What are the six ways an identity thief acquires information? (6 points)
5. How often should a person check his/her credit report? (1 point)
6. Who are the three credit reporting agencies? (3 points)
7. Where should outgoing mail be deposited? (1 point)
8. What are three ways to prevent a wallet or pocketbook from being stolen? (3 points)
9. What are three types of information found on a bill? (3 points)
10. Calling cards should include what type of number for safety? (1 point)

11. A unique password includes what type of combination? (1 point)
12. What are two types of information which can be found on work records? (2 points)
13. What should a person do if he/she receives a pre-approved credit card and does not want to use it? (1 point)
14. Name three ways to prevent bank account information from being used fraudulently. (3 points)
15. Why is a social security number also known as the “key to a person’s identity?” (1 point)
16. Why are credit and debit cards easy to use fraudulently? (1 point)
17. Identify five ways to prevent ATM, credit, or debit cards from being used fraudulently. (5 points)
18. What are the seven tips for shopping online safely? (7 points)
19. If a person is a victim of identity theft, what are the six steps to follow? (6 points)
20. What dollar amount is a person liable for with unauthorized credit card charges? (1 point)
21. If an ATM or debit card is stolen, what does an individual’s liability depend upon? (1 point)
22. What two things should a person do if his/her checks are stolen? (2 points)

IDENTITY THEFT INTERVIEW QUESTIONS

Name_____

Date_____

Class_____

Directions: Interview an adult using these questions. Discuss with them why this information is important for them to know. Following the interview, write a one page essay about the identity protection knowledge of the interviewee using the interview rubric.

1. What information do you have in your wallet or purse a thief can use?
2. How can a thief use this information?
2. What is identity theft?
3. What is a credit report?
4. Do you have a list of your credit card numbers? If so, is it kept in a secure place?
5. Do you keep your ATM, credit and debit card receipts?
6. Do you check the receipt charges with the charges on your monthly statement?
7. Do you check your monthly statement for fraudulent charges?
8. Do you destroy pre-approved credit card applications?
9. Do you mail your bill payments in a post office mailbox?
10. Do you use your credit card for unsolicited phone purchases?
11. Do you use a secure browser for Internet purchases?

IDENTITY THEFT INTERVIEW ESSAY RUBRIC

Name: _____

Date: _____

Directions:

- Participant must write a one page, typed, double-spaced, 12-font with 1-inch margins essay on the identity protection knowledge of the individual they interviewed.

	Exemplary - 3	Satisfactory - 2	Unsatisfactory - 1	Rating	Weight	Score
Content	The participant identifies and explains at least three reasons why the interviewee does or does not have a strong knowledge about identity protection.	The participant identifies three reasons why the interviewee does or does not have strong knowledge about identity protection.	The participant identifies less than three reasons why the interviewee has strong knowledge about identity protection.		3	
Content	The report is well organized and contains accurate quotations and facts taken from the interview.	The report contains accurate facts taken from the interview.	The report is lacking facts and quotations from the interview OR the quotes and facts are not accurately reported.		3	
Writing Skills	Sentences are fluent and effective. Very few errors in mechanics, punctuation, and word usage.	Sentences are usually controlled. There are minor errors in mechanics, punctuation, and word usage.	Sentences are generally adequate. There are lapses in mechanics, punctuation, and grammar.		2	
Presentation and Completion	Assignment is easily read and neatly assembled with an introduction, body and conclusion. Presentation quality is excellent.	Assignment is adequate. Answers may be missing, incomplete or too brief. Presentation quality is adequate.	Assignment is incomplete. Answers show lack of attention. Presentation is sloppy.		2	
				Total Points Earned		
				Total Points Available		30
				Percentage		

IDENTITY THEFT BROCHURE RUBRIC

Name _____

Date _____

Class _____

Directions:

1. Participants must create a brochure that will educate others about identity theft.
2. This brochure may be created by both writing and drawing information and pictures on a piece of 8 and ½ by 11 paper or by creating a brochure on the computer.
3. Your brochure must include answers to 4 of the following 6 questions in either bulleted or paragraph form:
 - a. What is identity theft?
 - b. How can thieves get an individual's information?
 - c. What should an individual do if they are a victim of identity theft?
 - d. How can individuals protect themselves?
 - e. If an individual's identity is stolen, what are they liable for?
 - f. What are the three credit reporting agencies and why are they important?

	Exemplary - 3	Satisfactory - 2	Unsatisfactory - 1	Rating	Weight	Score
Content	The participant identifies and answers all four questions assigned and the answers are correct.	The participant answers three or more of the six questions assigned with correct or incorrect answers.	The participant answers less than three of the six questions assigned with correct or incorrect answers.		3	
Creative	The brochure was creative with color added and a catchy title.	The brochure lacked creativity, color, or a catchy title.	The brochure has little or no color, is missing a title, and has little or no creativity.		3	
Grammar	Sentences are fluent and effective. Very few errors in mechanics, punctuation, and word usage.	Sentences are usually controlled. There are minor errors in mechanics, punctuation, and word usage.	Sentences are generally adequate. There are lapses in mechanics, punctuation, and grammar.		2	
Organization	Assignment is easily read and neatly assembled.	Assignment is adequate. Answers may be missing, incomplete or too brief.	Assignment is incomplete. Answers show lack of attention.		2	
				Total Points Earned		
				Total Points Available		30
				Percentage		