

CREDIT

ACTIVITY 7



Identity Theft

RECOMMENDED TIME

Allow 50-60 minutes. Required time may vary depending on the audience.

OBJECTIVES

Participants will:

- Define identity theft.
- Recognize the primary ways that identity theft occurs.
- Understand the immediate steps to take if your identity has been stolen.
- Understand how to manage personal information to keep it safe.

MATERIALS NEEDED

- Overhead projector and screen*
- Overhead transparency, flipchart, or white board
- Activity handouts

ADVANCE PREPARATION NOTES

Review the activity plan. Think about the audience, and decide whether to present the total activity or to use parts of this activity in combination with other activities.

For clarity, use print instead of script when writing on a flipchart, white board, or transparency.

The suggested dialogue in the delivery notes does not always mirror the wording on a transparency. Try to vary the dialogue, rather than reading transparencies verbatim.

This activity uses handouts. Have sufficient copies for all participants; a few extras provide good insurance.

* If an overhead projector isn't available, consider making photocopies of the overhead transparencies for handouts instead.

CREDIT

ACTIVITY 7 - DELIVERY NOTES



Identity Theft

Presentation Opening

- Welcome the participants.
- Introduce yourself briefly.
- If this is the first meeting with the class or group, do a brief round of introductions by everyone.
- When introducing yourself, print your name where participants can see and refer to it during the session. Some people may be a little nervous and may not remember your name. Just as you want to use their names, encourage them to call you by your name.

Activity Overview

Review the topics for discussion in this activity:

- Understand the growing problem of identity theft.
- Learn about several ways that identity theft can occur.
- Discuss important strategies to protect your personal information.
- Outline the steps to take if your identity has been stolen.

Write the term “identity theft” on the board, flipchart, or blank transparency.

Ask participants to define the term.

Ask participants how identity theft occurs.

Ask participants whether they or anyone they know has been a victim of identity theft, and ask them to share their stories if appropriate.

Debrief by showing “**Overhead 1: Identity Theft,**” and discussing the following talking points:

- The crime of identity theft is on the rise. Identity theft occurs when someone uses your personal identifying information (e.g., name, Social Security Number, date of birth) to either establish credit under your name or to take over an existing account that you established, without your authorization.
- Discuss the points on Overhead 1.
- Point out that anyone can have his or her identity stolen. Some individuals, such as those with common surnames and the elderly, may have an added risk.
- Fraudulent charges on your credit card, or having your card lost or stolen are equally frustrating to the consumer, but this does not mean that you are a victim of identity theft.

Visual Aids

Overhead 1 Identity Theft

CREDIT

ACTIVITY 7 - DELIVERY NOTES



Identity theft happens in a variety of ways. Distribute "**Handout 1: How Identity Theft Occurs**" and walk participants through it.

Separate participants into teams of two.

Read the two examples of *How Identity Theft Occurs*, below.

Have one participant take example A and the other, example B. Have them each discuss ways personal information could have been protected in each example.

Examples of How Identity Theft Occurs

- A. While checking your email, you notice a message from what appears to be your Internet Service Provider (ISP). The email message requests personal information so that your account can be updated. The message requests your name, Social Security Number, and mother's maiden name. In reality, the message is not from your provider. It belongs to someone who wants to get your information to steal your identity.
- B. As you are paying your monthly bills, you write the checks, toss the statements in the trash, and put the container out on the curb for the morning's trash pick-up. While you sleep, "dumpster divers" go through your trash looking for the papers you've thrown away. They find your name, address, phone number, utility service account numbers, credit card numbers, and your Social Security Number. Identity thieves can now use this information for fraudulent purposes.

Have participants share a few ideas about protecting personal data and then distribute "**Handout 2: How to Avoid Identity Theft**."

Discuss the following points:

- Ask participants for suggestions of additional ways to safeguard your personal information.
- Record this information on flipcharts.
- Some additional strategies might include not using your Social Security Number (SSN) as an identification number; never giving out your SSN, credit card number or other personal information over the phone, by mail, or on the Internet unless it is requested by a trusted source; memorize all your passwords and don't record them on anything in your wallet; and install a firewall and virus protection on your home computer.
- Ask participants to complete the bottom of Handout 2 by listing some things they can do to protect their personal information.

Visual Aids

Handout 1

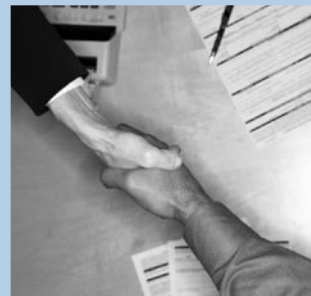
How Identity Theft Occurs

Handout 2

How to Avoid Identity Theft

CREDIT

ACTIVITY 7 - DELIVERY NOTES



Display “**Overhead 2: What to Do if your Identity Has Been Stolen**” and discuss the following:

- Contact the fraud departments of the three major credit bureaus to place a fraud alert on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts.
- Close the accounts that you know or believe have been tampered with or opened fraudulently.
- Contact all the creditors involved – Let them know that your accounts may have been used without your permission, or that new accounts have been opened in your name. If your accounts have been used fraudulently, ask that new cards and account numbers be issued to you. Check your billing statements carefully and report any fraudulent activity immediately.
- File a police report – Get a copy of the report to submit to your creditors and others that may require proof of the crime.
- File a complaint with the Federal Trade Commission (FTC) – The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Call the FTC’s Identity Theft Hotline: 1-877-IDTHEFT (438-4338). (Write this number on the flipchart paper.)
- Keep a record of your contacts – Start a file with copies of your credit reports, the police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties. Follow up on all phone calls in writing and send all correspondence via certified mail, with a return receipt requested. Keep all of your records in a safe place.

Closing

Thank everyone for their participation, and encourage them to return for additional sessions. If such sessions are planned, you might provide a “sneak preview” of any activities to come.

Visual Aids

Overhead 2

What to Do if your Identity Has Been Stolen

CREDIT

ACTIVITY 7 - OVERHEAD 1



IDENTITY THEFT

Identity theft occurs when someone uses your personal identifying information (e.g., name, Social Security Number, date of birth) to either establish credit under your name or to take over an existing account that you established, without your authorization.

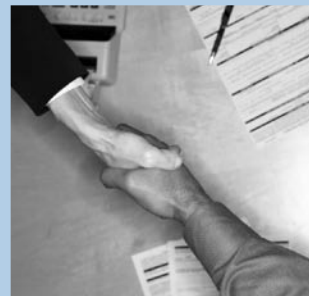
This information may include:

- **Social Security Numbers**
- **Name**
- **Address**
- **Date of birth**
- **Mother's maiden name**
- **Passwords**
- **PINs**

Many identity thieves use this personal information in order to open new credit card accounts, obtain loans and even mortgages in the victim's name, and/or take over existing accounts. In some cases, this personal identifying information can be used in the commission of a crime. Identity thieves are often people you know or come in contact with, but can also be complete strangers.

CREDIT

ACTIVITY 7 - HANDOUT 1



HOW IDENTITY THEFT OCCURS

Identity thieves use a variety of methods to gain access to your personal information. Some methods that identity thieves use include the following.

- They look for personal data by going through your trash, or the trash of businesses, looking for personal data in a practice known as “dumpster diving.”
- They steal wallets and purses.
- They may use personal information that you share on the Internet.
- They pose as legitimate companies or government agencies that you do business with in order to get your personal information.
- They steal your mail, including your bank statements, pre-approved credit offers, new checks, and tax information.
- They complete a “change of address form” to divert your mail to another location.
- They may place a virus on your computer that searches for bank account information that is followed by a PIN and/or a password. That information is ultimately sent to the identity thief without the victim’s knowledge.

CREDIT

ACTIVITY 7 - HANDOUT 2



HOW TO AVOID IDENTITY THEFT

1. Monitor your credit report. It contains your SSN, present and prior employers, a listing of all account numbers – including those that have been closed – and your overall credit score. If you become a victim of identity theft, you will catch the theft early by checking your credit report at least once per year. Order a free copy of your credit report by visiting www.annualcreditreport.com.
2. Don't give out personal information on the phone, through the mail, or on the Internet unless you initiate the contact or know the individual who initiated the contact. Thieves will pose as bank representatives, Internet service providers, government agents, and even ex-boyfriends or -girlfriends to get you to reveal personal information.
3. Protect your credit and debit cards. Whenever you receive a new card, sign it immediately. Don't loan it to anyone. Do not carry extra credit cards or other important identity documents except when needed.
4. Protect your mailbox. Remove your mail as soon after delivery as possible, and deposit outgoing mail in post office collection boxes.
5. Protect your wallet. Keep items with personal information in a safe place at home and do not share this information with friends or acquaintances. Don't carry your Social Security card in your wallet. Instead, memorize the number.
6. When creating passwords and PINs (personal identification numbers), do not use any numbers or codes that could easily be guessed by thieves.
7. Ensure your computer has appropriate anti-virus software that will detect and prevent keylogging viruses.
8. Notify your bank when you change your address or phone number.
9. Other suggestions: _____

List some things you will do to protect your personal information:

1. _____
2. _____
3. _____
4. _____
5. _____

CREDIT

ACTIVITY 7 - OVERHEAD 2



WHAT TO DO IF YOUR IDENTITY HAS BEEN STOLEN

If you think your identity has been stolen, take the following steps.

- Contact the three major credit bureaus.
(To report fraud: Equifax: 800-525-6285;
Experian: 888-397-3742; Trans Union: 800-916-8800)
- Close accounts.
- Contact all creditors involved.
- File a police report.
- Keep a record of your contacts.