

### PRIVACY PLEASE!

This leader's guide is designed to accompany the *Privacy Please!* teen guide. The leader's guide includes: learning objectives, background information, discussion questions, activities with accompanying handouts and visuals, a glossary, and a list of additional resources. The background information is meant to prepare leaders to both teach the unit and to provide lecture material to cover with the teens. Provide each teen a copy of the teen guide and ask them to read it *before* participating in the activities outlined in this guide.

The purpose of this unit is to help teens recognize identity theft methods that can be used to steal one's personal identity and identify the steps they can take to protect themselves against identity theft. You have an opportunity as a leader to help teens: recognize what identity theft is and the problems it can create, understand how to reduce the risks of identity theft, and know the steps to take if their personal information is stolen.

#### BACKGROUND INFORMATION

##### What is Identity Theft?

Identity theft is a crime in which someone steals another person's personal information and uses it for his/her own financial gain. Personal information can include a: Social Security number, credit card number, bank account information, or driver's license number (Qwest Communications, 2004). Thieves use the victim's identity and information to buy goods or services (such as renting an apartment), steal money from the victim's bank accounts, get new credit cards or loans using the victim's identity, or get a driver's license (Javelin Strategy and Research, 2008; Sherry, 2008).

#### Overall Learning Objectives

Teens will:

- Explain identity theft
- Recognize the types of information identity thieves are looking for and common methods thieves use to steal someone's personal information
- Identify steps that can be taken to protect personal information when using the internet and applying for jobs



Personal information includes:

- Social Security number
- Credit card number
- Bank account information
- Driver's license number
- Address
- Phone numbers
- Date of birth
- Mother's maiden name
- Student ID number & password



University of California  
Agriculture and Natural Resources  
Publication 8404

### *Did You Know?*

- Almost all studies agree that the top states in terms of identity theft victims per capita are: New York, California, Nevada, Arizona, Texas, and Washington. (Identity Theft Resource Center, 2007)
- 15% of all identity (ID) theft cases are committed by a close friend or a family member of the victim. (Foley & ITRC Teen Coordinators, 2006)
- The Federal Trade Commission (FTC) receives more complaints about identity theft than any other type of fraud. (FTC, 2005)

### **How serious is the problem?**

In 2007, 8.1 million American consumers were victimized at a total cost of \$45 billion (Javelin Strategy and Research, 2008). In addition to direct financial losses, identity theft victims may also face higher credit card fees, difficulty in finding a job, higher interest rates on loans, and battling collection agencies and issuers who refuse to clear records despite evidence substantiating the crime. Identity theft victims may also find themselves being sued or arrested for things they did not do. Resolution of identity theft is time consuming. In 2004, victims spent an average of 330 hours over 4–12 months recovering from this crime. The effects of identity theft can last as long as 10 years (Identity Theft Resource Center, 2007).

### **Teens are targeted more than other groups**

Identity thieves target teens and young adults more often than any other age group. According to the Federal Trade Commission, 29% of identity theft victims are between the ages of 18–29 (Federal Trade Commission, 2005). Teens' frequent use of the internet for purchases, social networking, on-line banking, and even blogging can put them at risk since they may not be aware of the potential problems or the need to protect themselves.

### **Teens are more vulnerable than others**

A 2004 *Summit on Protecting Teens from Identity Theft* found teens are particularly vulnerable to identity theft for several reasons (Qwest Communications, 2004):

- They have limited knowledge of financial transactions or credit reports.
- They are less educated about identity theft, prevention, and warning signs.
- Most have not established credit records that can be monitored, and as a result identity theft may go undiscovered for several years.
- They spend more time on the internet than other age groups and tend to be more careless about sharing their personal information online.
- They are less likely than others to check their credit reports and may not even be aware of their credit report and how important it is (Schonberger, 2005).

## Privacy Please



### Teens think it won't happen to them

Many teens and young adults—40% of those under age 25—believe they are more likely to be hit by lightning, to be audited by the IRS, or to win the lottery than be the victim of a computer security problem (The National Cyber Security Alliance, 2004, as cited in Qwest Communications, 2004).

In reality, about 70% of computer users face computer security threats such as viruses, phishing scams, and hacking, while the odds of being hit by lightning are 0.0000102%, according to the U.S. National Weather Service (BBC, 2004, as cited by Qwest Communications, 2004).

### Teens need information about identity theft so they can protect themselves

Identity theft can affect a teen's future ability to get a job or credit. To prevent identify theft, help teens to understand (Qwest Communications, 2004):

- Common forms of identity theft
- How to prevent it
- Warning signs that they have been victimized
- What to do if their identity is stolen

### Common Forms of Identity Theft

#### How do thieves steal personal information?

Identity thieves use many methods to get someone's personal information. They are continually coming up with new ways to get the information as old ones become more difficult to use. Theft can start with a lost or stolen wallet, mail taken from someone's mailbox, a data breach, a computer virus, phishing, a scam that tricks someone into revealing personal information, or paper documents thrown out by an individual or business (Identity Theft Resource Center, 2008).

According to a recent survey, criminals get the majority of their information from stolen personal belongings, and through telephone calls (Javelin Strategy and Research, 2008). Some ways they can get the information include (Consumer Action, 2006):

- Stealing a person's mail or completing change of address forms to divert a person's mail (such as credit card or bank statements) to another address.

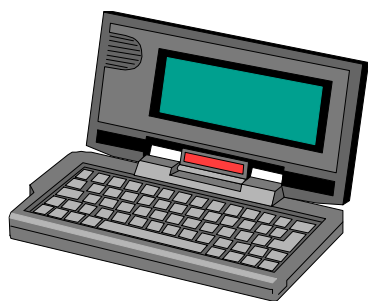


### *Did You Know?*

- Theft is the number one crime on college campuses. Teens need to be careful about the personal information they keep on their computers and the security measures they take to protect access to that information. (U.S. Dept. of Ed., 2008)



# Privacy Please



Hacking in regards to privacy means that an unauthorized person broke into a victim's computer and files with the intent to steal private information stored on that computer.

- Looking in trash bins to find documents containing personal information that were thrown out by individuals or businesses, (referred to as *dumpster diving*).
- Watching or listening as someone punches in their password or Personal Identity Number (PIN) or says their credit card number, (referred to as *shoulder surfing*).
- Stealing an unattended wallet, purse, backpack, cell phone, or laptop computer.
- Finding the information in someone's home.
- Hacking into a computer or redirecting the users to bogus websites, where they unsuspectingly enter their information.
- Trying to get email users to respond to "phishing" e-mails which tricks them into giving confidential information.
- Using the telephone to capture someone's account numbers and PIN codes. This is called "voice phishing" or "vishing" for short. A person is sent an e-mail, but instead of being asked to click on a link to go online, he or she is asked to call a phone number. Typically the e-mail will say there is trouble with the person's account and he has to call to straighten it out. But the phone number is not legitimate and personal information is captured as it is entered into the fraudulent phone system.
- Stealing databases from businesses, schools and other organizations that have personal information in their files.

### **What do thieves do with a stolen identity?**

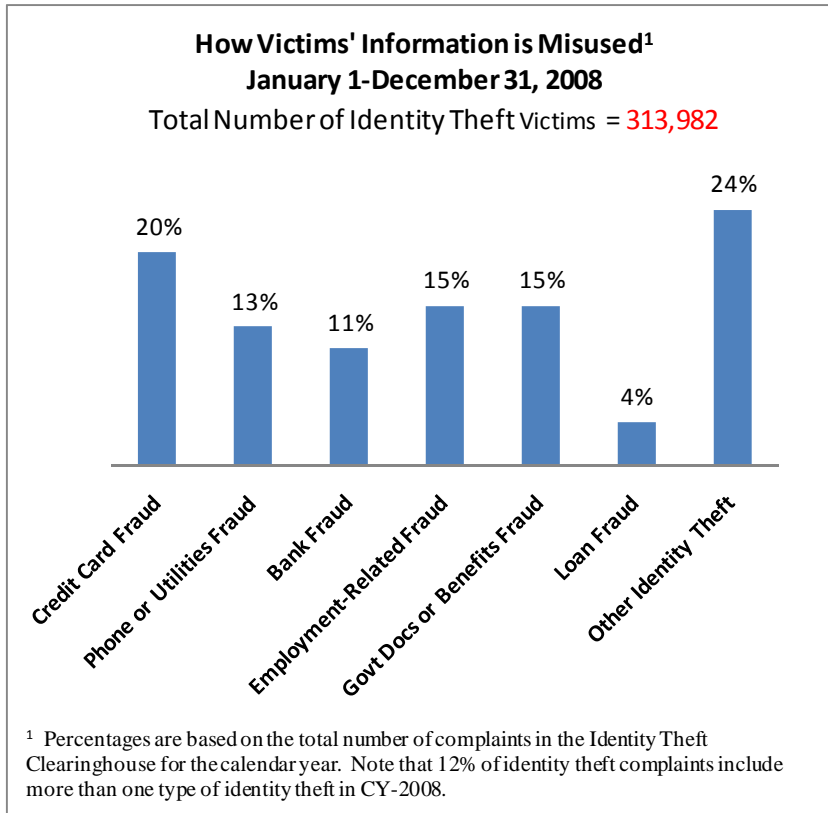
Basically, thieves use stolen personal information five ways (Javelin Strategy and Research, 2008; Sherry, 2008):

1. To purchase goods or services
2. To steal money from the victim's account(s)
3. To open new accounts in the victim's name
4. To commit other crimes
5. To sell information to other criminals

# Privacy Please



The following graph shows the percentage of misuse by type of identity fraud or other activity.



Source: Federal Trade Commission, released 2/26/09

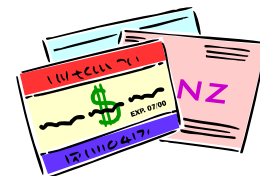
Following are descriptions of common ways identity thieves use stolen personal information for their own benefit (downloaded on 7/16/09 from [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft))

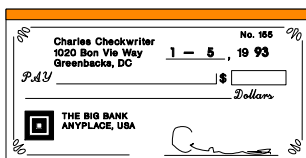
### Credit card fraud occurs when:

- A new credit card account is opened in the victim's name using the thief's address. The thief uses the card but doesn't pay the bills. The delinquent account appears on the victim's credit report. Since the victim doesn't receive the bills, it may be some time before the victim realizes there's a problem.

### Phone or utilities fraud occurs when:

- A new phone is opened in the victim's name, or charges appear on the existing account.
- The victim's information is used to get utility services like electricity, heating, or cable TV.





### Privacy Tips

- Watch your cell phone. An identity theft could steal your phone and e-mail your family asking for personal login information. Be safe, never send login or account information by text messaging.
- Don't carry your Social Security card in your wallet or purse. Memorize your Social Security number and leave your card in a safe place at home. (Consumer Action, 2006)
- Watch your wallet or purse at all times. At work or school, keep your purse in a locked drawer or cabinet. Don't hang your purse on your chair in restaurants. (Consumer Action, 2006)

### Bank/fraud occurs when:

- Counterfeit checks using the victim's name or account number are created.
- Bank accounts are opened in the victim's name and bad checks are written.
- The victim's automated teller machine (ATM) or debit card is cloned and electronic withdrawals are made in the victims' name, draining his or her accounts.
- A loan is taken out in the victim's name.

### Employment-related fraud occurs when:

- The victim's Social Security number is used to get a job
- A thief obtains employment in businesses such as doctors offices or banks to gain access to customer or patient records with personal and financial data.

### Government documents or benefit fraud occurs when:

- A driver's license or official ID card are issued in the victim's name, but with the thief's picture.
- The victim's name and Social Security number are used to get government benefits, such as Medicare (*known as MediCal in California*).

### Loan fraud occurs when:

- A thief uses a victim's name and good credit history to get a consumer loan or mortgage for themselves.

### Other fraud occurs when:

- A house is rented or medical services are secured using the victim's name.
- The victim's personal information is given to police during an arrest. When the thief doesn't show up for their court date, a warrant for arrest is issued in the victim's name.

### Preventing & Reducing Risk of Identity Theft

Although no one can prevent identity theft, there are steps teens can take to reduce the risk of being victimized. The *Summit on Protecting Teens from Identity Theft* recommended five tips for teens (Qwest Communications, 2004):

1. **Don't be intimidated.** If a coach, teacher, or youth group leader asks for a Social Security, driver's license, or credit card number do not give out the information and refer them to a parent or guardian.

## Privacy Please



2. **Guard your personal information.** Use passwords to protect laptops, cell phones, pagers, and MP3 players. Don't store personal information on these or other devices. Be cautious when throwing away papers with personal identifying information. Shred them with a cross-cut shredder if possible.
3. **Check it out.** Starting at age 18, request and monitor credit reports at least once a year to spot any unauthorized use of personal information. Everyone can get a free credit report yearly at [www.annualcreditreport.com](http://www.annualcreditreport.com). Also, regularly check bank and credit card statements for unusual or unapproved use.
4. **It's OK to say NO.** Don't loan out credit cards or any form of personal identification such as a driver's license or passport to anyone—not even a best friend, significant other, or sibling.
5. **Protect your Social Security number.** Don't give out a Social Security number when applying for a job—it's not necessary since the employer doesn't need that information until a job is offered. And don't put your Social Security number on your driver's license. Leave your Social Security card in a safe place at home. Don't carry it in your wallet where it could be lost or stolen.

### Online Shopping

Shopping online can be easy and economical. Follow these steps to assure it is a safe experience as well (OnGuardOnline.gov, 2008).

- Know who the seller is. Verify the seller's physical address and phone number before buying.
- Know what is being purchased. Read the product description carefully, especially the fine print.
- Know how much it will cost. In addition to the price of the item, consider shipping and handling charges.
- Charge it. Use a credit card for the purchase to ensure protection under the Fair Credit Billing Act.
- Know the terms. Find out about return policies and delivery dates before buying.

### *Did You Know?*

- Limit how financial institutions share personal financial information with other companies by "opting out." This will cut down on unsolicited credit offers.
- Opt-out is the process of notifying businesses and telemarketers that a person does not want to receive solicitations regarding their products.
- Financial institutions send a privacy notice once a year with statements or as a separate mailing. The notice describes the type of personal information the company collects and how that information is used. Read these notices to learn how private information is used. To opt out, follow the company's instructions—such as call, return a form, or go online.
- Shop around for a financial institution with an acceptable privacy policy. This is a company's guideline for collecting and using its customers personal information. (FTC, 2003)

## Did You Know?

- For more information and tips to help teens protect themselves from identity theft go to the Identity Resource Center at <http://www.idtheftcenter.org/index.html>. Information includes *Teen Fact Sheets* about identity protection when connecting to the internet, blogging, file sharing and peer-to-peer software safety, and tips for job seekers.
- For a detailed list of ways for people of all ages to protect their identity, see *Fact Sheet 17: Reducing the Risk of Identity Theft* available from the Privacy Rights Clearinghouse at <http://www.privacyrights.org/fs/fs17-it.htm#reduce>



- Keep records. Print and save records of all transactions, including product description, online receipt, and e-mail with the seller.
- Be sure the website is secure before providing financial information (FTC, 2008).
- Enter payment information each time, rather than storing data on a retailer's website (Susswein, 2008a).
- Before buying, read the company's privacy policy to find out how your personal data will be shared with other groups, such as marketers (Susswein, 2008b).
- Review website privacy seals. Look for merchants displaying privacy seals such as TRUSTe or BBBOnline, which means that a company meets high privacy standards (Susswein, 2008a).

## Warning Signs of Possible Identity Theft

Teens who recognize the signs that their identity may have been stolen can act quickly to limit the damage. Teens are advised to obtain a current credit report and review it for unauthorized use if any of the following occur:

- Apply for a driver's license and find out another one has already been issued under their name (If so, they might also have a few traffic tickets.)
- Applications for student loans, credit cards, or apartment rental are denied for no apparent reason
- Unsolicited credit card offers in their name (Mailing lists are created from those who already have credit histories.)
- Get credit collections calls or letters in the mail
- A number of telemarketers call asking to speak with them by name (Qwest Communications, 2004)

### **Other warning signs**

Unfortunately, many people don't find out their identity has been stolen until some damage has already been done. Any of the following events may indicate a problem:

- Accounts listed on credit report that teen didn't open
- Charges on account(s) that can't be explained
- Fraudulent or inaccurate information on credit reports, including accounts and personal information, like a Social Security number, address(es), name or initials, and employers' names



## Privacy Please



- A missing bill or statement could mean an identity thief has taken over an account and changed the billing address to cover his/her tracks. Follow up with creditors if bills don't arrive on time
- Receiving credit cards that weren't applied for
- Being denied credit, or being offered less favorable credit terms, like a high-interest rate, for no apparent reason
- Getting calls or letters from debt collectors or businesses about merchandise or services not purchased (Federal Trade Commission, downloaded 8/18/09 from [www.ftc.gov](http://www.ftc.gov))

### What to Do If Identity Theft Occurs

Act quickly to prevent or limit damage if:

- A notice is received from a company indicating personal information has been compromised
- There is risk of identity theft because a wallet has been stolen
- Account information has been given in response to what may be a phishing scam
- A collection notice is received

The Federal Trade Commission recommends the following steps (Federal Trade Commission, 2008) to protect against identity theft:

#### **1. Place a fraud alert on the credit file.**

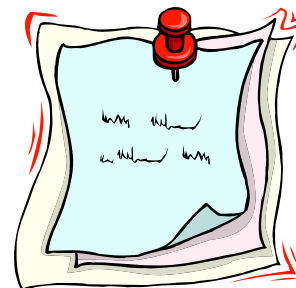
Put a "fraud alert" on the credit file by calling one of the three credit reporting agencies, which will notify the others. A fraud alert requires creditors to take steps to verify the identity of the credit applicant's identity. While this is helpful, there are limitations. A creditor still may not detect the applicant is not who he or she claims to be. Some creditors such as apartment managers or telephone companies do not use credit reports in extending credit.

#### **2. Get a free credit report.**

Placing the fraud alert in a file entitles the person to one free copy of their credit report from each consumer credit reporting agency. When the credit reports are received, check each one, to see if there are:

### *Did You Know?*

- There are three major credit reporting agencies :
  - ⇒ **Equifax:**  
PO Box 105873  
Atlanta, GA 30348  
(800) 685-1111  
[www.equifax.com](http://www.equifax.com)
  - ⇒ **Experian:**  
PO Box 20002  
Allen, TX 75013  
(888) 397-3742  
[www.experian.com](http://www.experian.com)
  - ⇒ **Trans Union:**  
PO Box 390  
Springfield, PA  
19064-0390  
(800) 888-4213  
[www.transunion.com](http://www.transunion.com)
- Consumers are entitled to a free copy of their credit report each year from each of the three credit reporting agencies. All reports can be requested from [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-fact-act



*Did You Know?*

- You can access the FTC's online complaint form at <http://www.ftc.gov> (see Identity Theft), or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338) TTY: 1-866-653-4261.
- The FTC's identity theft site has information about resolving specific identity theft problems including:
  - bank accounts
  - credit cards
  - student loans
  - criminal violations
  - others types of fraud (<http://www.ftc.gov/bcp/edu/microsites/idtheft>)

**Opening Discussion Questions**

- Share a story of someone who has been a victim of identity theft.
- What are the different types of identity theft?
- How does identity theft affect someone's life?
- What can you do to reduce risk of identity theft?



- Unsolicited credit inquiries
- Unfamiliar accounts
- Unexplained charges on existing accounts

Also verify that all personal information, such as the Social Security number, address(es), name or initials, and employers are correct. If there is fraudulent or inaccurate information, have it removed (Federal Trade Commission, 2008).

**3. Close accounts that have been compromised.**

If credit reports indicate credit or financial accounts have been misused or opened fraudulently, close the accounts. As soon as possible, contact the Fraud Department of each company for assistance and then follow-up the call with a written request. Open new accounts and choose new passwords. Keep records of all calls and correspondence.

**4. File a report with the Federal Trade Commission.**

Complete the Federal Trade Commission's (FTC) online complaint form and print copies to keep for personal records and to give to the police or other local law enforcement agencies. Although the FTC generally does not investigate individual consumer complaints, the complaint form can be used as documentation for certain protections. These protections include removing the fraudulent information from the credit file, preventing calls from creditors/debt collectors, and allowing placement of an extended fraud alert. The information consumers submit goes into a national database used by law enforcement.

**5. File a police report.**

File a report with the local police or law enforcement agency where the fraud took place. Give them a copy of the FTC Complaint Form, and get a copy of the police report to use when disputing the fraudulent accounts and debts created by the identity thief.

# Privacy Please



## ACTIVITY ONE: WHAT IS IDENTITY THEFT?


*Estimated Activity Time: 60–75 minutes*

In this activity, teens will learn what identity theft is, why they are vulnerable, how to recognize the different types of identity theft, and what thieves do with stolen identity information.

### Getting Ready Checklist

- Make one copy of Handout #1a, #1b, #1c, #1d, or #1e for each group

### Doing the Activity

1. Review the “What is Identity Theft?” section on pp. 1–3 of the leader’s guide background information with teens. Include the following points:
  - Identity theft is a crime in which someone steals another person’s personal information and uses it for their own financial gain
  - 8.1 million Americans were victims of identity theft in 2007
  - Identity theft has very negative effects on the lives of victims
  - Teens are targeted for identity theft more than other groups
  
2. Download and show teens all or portions of the 11-minute *Identity Theft: Stolen Futures* video produced by the Identity Theft Resource Center. Go to:  [http://www.idtheftcenter.org/artman2/publish/t\\_facts/Teen\\_Video.shtml](http://www.idtheftcenter.org/artman2/publish/t_facts/Teen_Video.shtml). Discuss what teens thought about the video.
  - What did you learn about identity theft?
  - What surprised you about the types of identity thefts?
  - Who could be an identity thief?

## Learning Objectives

- Teens will understand what identity theft is
- Teens will understand they are at risk of identity theft
- Teens will be able to recognize the different types of identity theft
- Teens will understand what can happen when financial information is stolen

## Supplies Needed

- *Privacy Please* teen guide
- Downloaded video “Identity Theft: Stolen Futures” [http://www.idtheftcenter.org/artman2/publish/t\\_facts/Teen\\_Video.shtml](http://www.idtheftcenter.org/artman2/publish/t_facts/Teen_Video.shtml)
- Handouts #1a–#1e (pp. 37–41)



## Privacy Please



- Who could be an identity theft victim?
  - Name two agencies that can provide free help if you're a victim of identity theft.
3. Ask teens to take the “How High is My Risk?” quiz on p. 2 of the *Privacy, Please!* teen guide. Discuss how they did as a group.
  4. Divide teens into small groups of three to four and give each group one of the fraudulent e-mails, Handouts #1a–#1e. These are actual phishing or pharming e-mails, including the misspellings, that have had company names and e-mail addresses altered. Have teens answer the questions in their groups. After 10 minutes have the groups report to the entire group. (Handouts #1a–#1e, pp. 37–41)



~The assessment tools provided with each leader's guide are intended for the leaders to use at their discretion. Depending on the group of teens, the leaders may want to use the assessments as additional activities, homework, or as a means to determine a formal grade for completing the unit.

# Privacy Please



## ACTIVITY TWO: IDENTITY THEFT—REDUCING THE RISK

*Estimated Activity Time: 45–60 minutes*

In this activity, teens will evaluate two case studies to learn how to reduce the risk of identity theft. The first case study is about a teen setting up a blog or social networking site. The second case study is about a teen applying for a job. Teens will determine what was done right and what could be improved to reduce risks of identity theft.

### Getting Ready Checklist

- Copy Visuals #1, #2a and #2b to display
- Set up projector
- Make copies of Handouts #2 and #3
- Paper, different color highlighters/pencils/pen, whiteboard and markers
- Computers with online capabilities if Extend the Lesson activities will be used

### Doing the Activity

1. Review the “Preventing & Reducing Risk of Identity Theft” section on pp. 6–7 of the leader’s guide background information. Emphasize the five tips for teens by showing Visual #1 to reduce their risk of identity theft. (Visual #1, p. 29)
2. Ask teens if they can think of other ways to protect themselves from identity theft.
3. Ask teens what blogs or social networking sites they use. Ask them what steps they usually take to protect their confidential information. Encourage them to share why it is important to keep their information private.

### Learning Objectives

- Teens will learn about the ways to reduce the risk of identity theft

### Supplies Needed

- Handout #2 (p. 42)
- Handout #3 (p. 43)
- Visual #1 (p. 29)
- Visual #2a and #2b (pp. 30–31)
- Answer Key for Handout #2 (p. 46)
- Answer Key for Handout #3 (p. 47)

### Extend the Lesson Supplies

- Handout #4 (p. 44)
- Computers with online capabilities
- Printer
- Poster board
- Markers


### Related Money Talks Online

#### Games:

- To Shred or Not to Shred
- Privacy Match-Up  
(*These games are currently in development. A web address will be added when the games are posted.*)

## Privacy Please



4. Divide teens into groups of two to four and distribute Handout #2 to each teen. Explain that the handout is a case study about Lee who is setting up a blog on a social networking site. Give the groups time to review Handout #2 and ask groups to list the things Lee did right and the things he could have done to reduce the risks of identity theft. (Handout #2, p. 42)
5. Once the groups have completed reviewing and discussing the handout, have them share their lists with members of the entire group. Encourage teens to have an open discussion about the case study. (Answer Key for Handout #2, p. 46)
6. Next, ask teens if any of them have applied for a job by using a paper application or if they have applied online. Encourage them to share the information that was asked of them and how they would now fill out the application differently to reduce the risk of identity theft. Show teens Visual #2, a sample job application, to stimulate discussion. (Visual #2a and #2b, pp. 30–31)
7. Distribute Handout #3 and explain to the teens that the handout is a case study about Kesha applying for a job. Give the groups time to review Handout #3 and ask them to list the things Kesha did right and the things she should have done to reduce the risks of identity theft. (Handout #3, p. 43)
8. Once the small groups have completed reviewing and discussing the handout, have them share their lists with the larger group. Encourage teens to have an open discussion about this case study. (Answer Key for Handout #3, p. 47)
9. *Extend the Lesson—Privacy Policies and Me: Understanding a Website Privacy Policy*  
 Ask teens to read, “How to Read a Privacy Policy” at: [http://www.oispp.ca.gov/consumer\\_privacy/consumer/documents/pdf/cis6english.pdf](http://www.oispp.ca.gov/consumer_privacy/consumer/documents/pdf/cis6english.pdf)

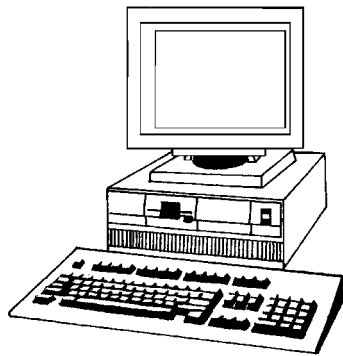
---

## Privacy Please

---



10. Ask teens to go to a website they have visited and print out the privacy policy (or assign them in groups to various types of websites: retail, bank, social networking, etc.) Have teens read the selected privacy policies and answer the questions on Handout #4. (Handout #4, p. 44)
11. Have each group discuss an item in the privacy policy to see if the information collected is appropriate for the type of site (i.e., retail site asking for Social Security number and birth date).
12. With the larger group, discuss the similarities and differences between the privacy policies and what steps they can take to reduce their risk of identity theft in the future.



-The assessment tools provided with each leader's guide are intended for the leaders to use at their discretion. Depending on the group of teens, the leaders may want to use the assessments as additional activities, homework, or as a means to determine a formal grade for completing the unit.





# Privacy Please



## ACTIVITY THREE: WARNING SIGNS OF POSSIBLE IDENTITY THEFT

*Estimated Activity Time: 60–90 minutes*

In this activity, teens will explore the various identity theft scams known by the federal government. In small group, teens will research a current identity theft scam and develop a skit to portray the scam, how victims are affected, warning signs of being a victim, and how to avoid the scam.

### Getting Ready Checklist

- Copy Handout #5 for each group
- Computers with online capabilities

### Doing the Activity

1. Summarize the “Common Forms of Identity Theft” section of the leader’s guide background information on pp. 3–6. Be sure to include the following facts.

Thieves get personal information by:

- Stealing mail or changing the address of someone’s mail
- Dumpster diving
- Shoulder surfing
- Finding information in someone’s home
- Computer hacking
- Redirecting victims to bogus websites (pharming)
- Voice phishing (vishing)
- Stealing databases

### Learning Objectives

- Teens will recognize the warning signs of identity theft scams that could affect them
- Teens will identify several ways to prevent or minimize identity theft
- Teens will become familiar with the resources available on the Federal Bureau of Investigation (FBI) and the Federal Trade Commission (FTC) websites

### Supplies Needed

- Handout #5 (p. 45)
- Computers with online capabilities



## Privacy Please



~The assessment tools provided with each leader's guide are intended for the leaders to use at their discretion. Depending on the group of teens, the leaders may want to use the assessments as additional activities, homework, or as a means to determine a formal grade for completing the unit.

Thieves use information to:

- Purchase goods or services
- Steal money
- Open new accounts in victim's name
- Sell to other criminals
- Commit other crimes

How Fraud Occurs:

- New credit card or loan is opened in victim's name
- New utilities are opened in a victim's name
- Counterfeit checks are used with victim's name and account information
- Victims' ATM or debit card is cloned
- Driver's license or other ID issued in victim's name with thief's picture
- Victim's name and Social Security card is used to get government benefits
- Victim's information is given to police when a thief is arrested



2. Divide teens into small groups of no more than three. Each group will conduct an online search of the newest and most common identity theft scams on the FBI <http://www.fbi.gov/> and FTC's <http://www.ftc.gov/> website. Each group will pick one scam that they feel is the most devastating and develop and perform a skit about it. The elements of the skit should include:

- Name and description of the scam
- How it affects the victim
- What are the warning signs
- How to avoid the risk or stop it

(Handout #5, p. 45)

3. Debrief each scam by summarizing:

- How the thief stole the personal information
- How the information was used
- Steps the victim now needs to take to restore his/her identity

# Privacy Please



## ACTIVITY FOUR: WHAT TO DO IF YOUR IDENTITY IS STOLEN

*Estimated Activity Time: 20–30 minutes*

In this activity, teens will become familiar with the five steps to take to minimize the impacts of identity theft on their personal lives. They have an opportunity to play a team game to identify these steps. Expand the lesson by adding a guest speaker or have teens serve as an expert panel on identity theft.

### Getting Ready Checklist

- |   |
|---|
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Copy Visuals #3a–3e to display</li> <li><input type="checkbox"/> Computers with online capabilities if Extend the Lesson activities will be used</li> </ul> |
|---|

### Doing the Activity

- Review with the teens the “What to Do if Your Identity is Stolen” background information on pp. 9–10 in this leader’s guide. Stress the importance of acting quickly by following these five steps:
  - Place a fraud alert in your credit file** by calling one of the three credit reporting agencies (that agency will notify the other two credit reporting agencies).
  - Get a free copy of your credit report**—placing a fraud alert entitles victims to one free copy of their credit report from each of the three credit reporting agencies which can be obtained at: [www.annualcreditreport.com](http://www.annualcreditreport.com).

### Learning Objectives

- Teens will identify steps to take to minimize the financial impacts after identity theft has occurred
- Teens will understand the importance of taking immediate action to address issues related to identity theft

### Supplies Needed

- Privacy Please* teen guide
- Visuals #3a–3e (pp. 32–36)

### Extend the Lesson

#### Supplies

- Computers with online capabilities

### Related *Money Talks* Online Games:

- To Shred or Not to Shred
  - What to Do If Your Identity is Stolen
  - Privacy Match-Up
- (These games are currently in development. A web address will be added when the games are posted.)*

- There are three major credit reporting agencies :

⇒ **Equifax:**  
PO Box 105873  
Atlanta, GA 30348  
(800) 685-1111  
[www.equifax.com](http://www.equifax.com)

⇒ **Experian:**  
PO Box 20002  
Allen, TX 75013  
(888) 397-3742  
[www.experian.com](http://www.experian.com)

⇒ **Trans Union:**  
PO Box 390  
Springfield, PA  
19064-0390  
(800) 888-4213  
[www.transunion.com](http://www.transunion.com)

- It is also possible to obtain a free yearly copy of credit reports at [annualcreditreport.com](http://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. Print the form from [ftc.gov/credit](http://ftc.gov/credit).

### Answer Key for Visuals #3a–3e

- a. fraud alert
- b. credit report
- c. Close accounts
- d. Federal Trade Commission
- e. police report

- **Close accounts that have been affected by identity theft** to prevent further problems.
- **File a report with the Federal Trade Commission**—using its online complaint form. This will require creditors to take extra steps to verify the applicant’s identity when applying for credit. Go to <https://www.ftccomplaintassistant.gov/> and click on “FTC Complaint Assistant” or call the FTC’s Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
- **File a police report** and give law enforcement officials a copy of the Federal Trade Commission complaint form completed online. Obtain a copy of the police report to assist in restoring your good credit.

2. To help teens identify the steps to take when an identity has been stolen, play the following *What to Do if Your Identity is Stolen* game. This game is played like the popular TV show where participants guess letters to fill-in blanks to solve a word puzzle.

- Display Visual #3a. (Visual #3a, p. 32)
- Ask a teen to guess one letter to fill-in the blanks and try to solve the puzzle.
- If the teen doesn’t guess a needed letter or is unable to solve the puzzle, give another teen an opportunity to guess a letter and solve the puzzle.
- Continue the game until the puzzle is solved. As time allows, repeat the game using Visuals #3b, #3c, #3d and/or #3e. (Visuals #3b–3e, pp. 33–36)



If computers with online capabilities are available, this game can be played online at [moneytalks4teens.org](http://moneytalks4teens.org).

## Privacy Please



### 3. *Extend the Lesson—Guest Speaker*

Invite an identity theft victim or law enforcement official to speak to the teens about identify theft, including the steps necessary to minimize the impact of identity theft.

### 4. *Extend the Lesson—Panel Discussion*

Five teens serve as experts on a panel to discuss what to do when a person is a victim of identity theft. Give each teen panel member one of the following topics to research and discuss:

- a. How to place a fraud alert on a credit file
- b. How to get a free copy of a credit report and what information is contained in the report
- c. How to close accounts that have been used fraudulently
- d. How to file a complaint with the Federal Trade Commission
- e. How to file and obtain a copy of a police report

To prepare the other teens to ask questions of the panel have them research cases on people who have been identity theft victims. They may do this:

- By speaking with people who have had their identity stolen; search the internet for stories, etc.
- Based on the information they gather, each teen prepares three questions to ask the panel.



~The assessment tools provided with each leader's guide are intended for the leaders to use at their discretion. Depending on the group of teens, the leaders may want to use the assessments as additional activities, homework, or as a means to determine a formal grade for completing the unit.

---

This publication has been anonymously peer reviewed for technical accuracy by University of California scientists and other qualified professionals. This review process was managed by the ANR Associate Editor for Youth Development.

To simplify information, trade names of products have been used. No endorsement of named or illustrated products is intended, nor is criticism implied of similar products that are not mentioned or illustrated.

ANR Publication 8404

©2009 by the Regents of the University of California  
Division of Agriculture and Natural Resources  
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the written permission of the publisher and the authors.

The University of California prohibits discrimination or harassment of any person on the basis of race, color, national origin, religion, sex, gender identity, pregnancy (including childbirth, and medical conditions related to pregnancy or childbirth), physical or mental disability, medical condition (cancer-related or genetic characteristics), ancestry, marital status, age, sexual orientation, citizenship, or status as a covered veteran (covered veterans are special disabled veterans, recently separated veterans, Vietnam era veterans, or any other veterans who served on active duty during a war or in a campaign or expedition for which a campaign badge has been authorized) in any of its programs or activities. University policy is intended to be consistent with the provisions of applicable State and Federal laws.

Inquiries regarding the University's nondiscrimination policies may be directed to the Affirmative Action/Staff Personnel Services Director, University of California, Agriculture and Natural Resources, 1111 Franklin Street, 6th Floor, Oakland, CA 94607, (510) 987-0096.

---

Money Talks...Should I Be Listening? Is a series of six teen and leader's guides designed for teens. The topics and subject matter content are based on the results of a survey completed by teens. The goals of these teen guides and leader's guides are to assist teens in 1) identifying their money spending and saving habits; 2) understanding the importance of long-term savings, and 3) developing savings plans that meet their lifestyles. Comments regarding these teen guides and leader's guides can be addressed to: Consumer Economics Department, University of California Cooperative Extension (UCCE), 135 Building C, Highlander Hall, Riverside, CA 92521. Authors: Patti Wooten Swanson, Margaret Johns, Keith Nathaniel, Charles Go, Brenda Roche, Shirley Peterson, Karen Varcoe and UCCE Money Talks Workgroup. 2009

---

## Privacy Please



---

### Additional Resources

- *California Office of Privacy Protection* provides consumer education and information on privacy issues. Fact sheets include tips for identity theft protection, how to read a privacy policy, and how to protect your computer.  
<http://www.privacy.ca.gov/>
- *Deter, Detect, Defend, AvoID Theft* The Federal Trade Commission offers this 10-minute video featuring advice from FTC leaders, law enforcement, and victims on how to deter, detect, and defend against identity theft. It features people of all ages talking about identity theft. Available in English and Spanish. Download free:  
<http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html#DVD>
- *Federal Bureau of Investigation (FBI)* This website contains background information and information on current federal investigations.  
[http://www.fbi.gov/publications/financial/fcs\\_report2006/financial\\_crime\\_2006.htm#Identity](http://www.fbi.gov/publications/financial/fcs_report2006/financial_crime_2006.htm#Identity)
- *Federal Trade Commission (FTC)* has a public education program kit “AvoID Theft: Deter, Detect, Defend,” available on a CD-ROM/DVD. Resources include a 10-minute video, PowerPoint slide set, and brochures. Most items can be downloaded from the website for free or order 100 free copies of the brochure.  
<http://www.ftc.gov/bcp/edu/microsites/idtheft/become-a-partner.html#DVD>
- *ID Theft and Account Fraud: Prevention and Cleanup* is a downloadable teacher’s kit from Consumer Action that includes a tri-fold brochure with tips for preventing ID theft, a 24-page leader’s guide with background information, a lesson plan, worksheets, PowerPoint training slides, and a quiz. Materials are available in English, Spanish, Chinese, Vietnamese, and Korean.  
[http://www.consumer-action.org/modules/articles/id\\_theft\\_account\\_fraud](http://www.consumer-action.org/modules/articles/id_theft_account_fraud)
- *ID Theft, Privacy, and Security*, Federal Trade Commission website includes fact sheets on various topics related to identity theft and consumer alerts.  
<http://www.ftc.gov/bcp/menus/consumer/data/idt.shtm>
- *Identity Theft Resource Center* is a national non-profit organization that focuses on identity theft. Their website has a section about teens and identity theft, examples of scams, quizzes and fact sheets (i.e., Blog Sense, File Sharing and Peer-to-Peer Software Safety). The Teacher Enrichment section has a vocabulary list, discussion questions, and suggested projects.  
<http://www.idtheftcenter.org/teen/teen.html>

## Additional Resources *cont.*

- *Identity Theft: Outsmarting the Crooks* is a DVD produced by the U.S. Treasury, featuring experts from the government and the private sector talking about the scope of the identity theft problem and steps people can take to protect themselves. View online at:  
[http://mfile.akamai.com/19311/wmv/yorkmedia.download.akamai.com/19311/wm.yorktelecom/Treasury/Public/2006/id\\_theft.asx](http://mfile.akamai.com/19311/wmv/yorkmedia.download.akamai.com/19311/wm.yorktelecom/Treasury/Public/2006/id_theft.asx)
- *Identity Theft: Stolen Futures* is an 11-minute teen oriented video produced by the Identity Theft Resource Center which introduces the importance of protecting against identity theft. Download for free:  
[http://www.idtheftcenter.org/artman2/publish/t\\_facts/Teen\\_Video\\_printer.shtml](http://www.idtheftcenter.org/artman2/publish/t_facts/Teen_Video_printer.shtml)
- *Leave me alone: Your privacy online—and offline* is a Consumer Action publication containing tips on how to safeguard your privacy.  
[http://www.consumer-action.org/english/articles/leave\\_me\\_alone\\_eng\\_2008](http://www.consumer-action.org/english/articles/leave_me_alone_eng_2008)
- *Money Talks* is a financial literacy website for teens available in both English and Spanish. It contains downloadable versions of money management teen guides, interactive games, simple exercises, videos and links to other financial websites. Teachers/leaders have access to a special section of the site containing leader's guides for each unit, research articles, and additional links.  
<http://moneytalks4teens.org>



## References

- California Office of Information Security and Privacy Protection. (2008). How to read a privacy policy. Retrieved June 3, 2008, from [http://www.oispp.ca.gov/consumer\\_privacy/default.asp](http://www.oispp.ca.gov/consumer_privacy/default.asp)
- Consumer Action. (2006). ID Theft & Account Fraud Leader's Guide: Strategies for prevention and clean up. Retrieved May 28, 2008, from [http://www.consumer-action.org/english/articles/id\\_theft\\_account\\_fraud\\_leaders\\_guide/](http://www.consumer-action.org/english/articles/id_theft_account_fraud_leaders_guide/)
- Federal Trade Commission. Fighting back against identity theft. Retrieved May 20, 2008, from <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- Federal Trade Commission. (2003). Getting Credit: What You Need to Know About Credit. Retrieved June 3, 2008, from <http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre32.shtm>
- Federal Trade Commission. (2005). National and state trends in fraud and identity theft, January to December 2004. Retrieved May 28, 2008, from [http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse\\_2004.pdf](http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2004.pdf)
- Federal Trade Commission. (2008). On Guard Online: Your Safety Net, Online Shopping, Quick Facts. Retrieved February 24, 2009, from <http://www.onguardonline.gov/topics/online-shopping.aspx>
- Federal Trade Commission. (2009). Consumer Sentinel Network Data Book for January—December 2008. Retrieved from <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf>
- Foley, L., & ITRC Teen Coordinators. (2006). Fact Sheet 127 - Blog Sense. Retrieved June 3, 2008, from [http://www.idtheftcenter.org/artman2/publish/t\\_facts/Fact\\_Sheet\\_127.shtml](http://www.idtheftcenter.org/artman2/publish/t_facts/Fact_Sheet_127.shtml)
- Identity Theft Resource Center. (2007). Facts and statistics: Find out more about the nation's fastest growing crime. Retrieved May 29, 2008, from [http://www.idtheftcenter.org/artman2/publish/m\\_facts/Facts\\_and\\_Statistics.shtml](http://www.idtheftcenter.org/artman2/publish/m_facts/Facts_and_Statistics.shtml)
- Identity Theft Resource Center. (2008). Retrieved May 28, 2008, from <http://www.idtheftcenter.org/>

References *cont.*

- Javelin Strategy and Research. (2008 ). New research confirms identity fraud is on decline. Retrieved May 20, 2008, from <http://www.javelinstrategy.com/2008/02/11/new-research-confirms-identity-fraud-is-on-decline/>
- Qwest Communications. Don't get ripped off! Identity theft tips for teens. Retrieved May 28, 2008, from <http://www.qwest.com/highwayqwest/identitytheft/index.html>
- Qwest Communications. (2004). *2004 Summit on protecting teens from identity theft: Key findings*: Qwest Communications.
- Schonberger, J. (2005). Emerging identity theft market targets teens as newest niche. *Journal*. Retrieved from [http://www.pbs.org/newshour/extra/features/july-dec05/idtheft\\_8-29.html](http://www.pbs.org/newshour/extra/features/july-dec05/idtheft_8-29.html)
- Sherry, L. (2008, Spring ). Make safety first online. *Consumer Action News*, 1 & 4.
- Susswein, R. (2008a, Spring). It's safe and easy to pay online if you know the rules. *Consumer Action News*, 2 & 5.
- Susswein, R. (2008b). Mobile commerce makes an appearance in the U.S. *Consumer Action News*, Spring, 1.
- U.S. Department of Education, Office of Postsecondary Education. The Campus Security Data Analysis Cutting Tool. Retrieved February 25, 2009, from <http://ope.ed.gov/security/GetAggregatedData.aspx>

## Privacy Glossary

**Account Redirection** A crime where thieves go to the post office and fill out a change of address form for someone else so the victim's mail is sent to the thief.

**Computer Spyware** Software that can record a website history and everything that is typed in. Thieves use the information to commit crimes.

**Credit Report** A file maintained by consumer reporting agencies/credit bureaus that contains a record of a consumer's credit payment history. A consumer has a credit record on file at a credit bureau if he/she has ever applied for a credit or charge account, a personal loan, insurance, or a job.

**Credit Reporting Agency** An agency (sometimes known as a credit bureau) that assembles credit and other information on consumers to help companies determine their creditworthiness. The three major national credit bureaus are Equifax, Experian (formerly TRW), and Trans Union.

**Dumpster Diving** Looking in trash bins to find documents containing personal information that were thrown out by individuals or businesses.

**Fraud Alert** A written notice filed with a credit reporting agency that requires creditors to take certain steps to verify the identity of anyone who applies for credit in the consumer's name.

**Identity Theft** A crime in which someone steals an individual's personal information such as their Social Security number, credit card number, bank account information, or driver's license number and uses it for their own financial gain.

**Opt-out** The process of notifying businesses and telemarketers that a person does not want to receive solicitations regarding their products.

**Password** A secret word or string of characters that is used to prove identity or gain access to a database.

**Pharming** (pronounced "farming") A crime where thieves create fake websites that look like banks or online store websites and buy domain names similar to the banks' or stores' web address. When a victim accidentally types in the wrong web address, the thief steals the victim's username and password.

## Privacy Glossary *cont.*

**Phishing** (pronounced “fishing”) E-mail messages enticing readers to reveal personal information.

**PIN (Personal Identification Number)** A number, selected by the individual, used to access his/her bank account through an ATM or debit card.

**Privacy Notice** A notice sent to account holders yearly to inform them of the type of personal information the company collects and how that information is used.

**Privacy Policy** A company’s guidelines for collecting and using their customers personal information.

**Shoulder Surfing** Watching or listening as someone types in or says an account number, password or PIN.

**Skimming** A thief copies a victim’s credit card number or uses a card reader in an ATM machine, then uses the victim’s credit card or ATM card to make purchases or withdraw money from the victim’s account.

**Username** An identification for a user of computing equipment; can also be known as a screen name or handle.

**Vishing** A shortened name for voice phishing.

**Voice Phishing** A phone call enticing people to reveal their account number and PIN code.

**Wireless Hacking** Thieves use unsecured wireless computer or cell phone connections to steal a victim’s personal information.



## 5 Tips for Teens to Help Reduce the Risk of Identity Theft

1. Don't be intimidated.
2. Guard your personal information.
3. Check out your credit report.
4. It's OK to say 'NO'.
5. Protect your Social Security number.



# Privacy Please

## APPLICATION FOR EMPLOYMENT

**PERSONAL INFORMATION**

DATE OF APPLICATION: \_\_\_\_\_

Name:

\_\_\_\_\_ Last First Middle

Address:

\_\_\_\_\_ Street (Apt) City, State Zip

Alternate Address:

\_\_\_\_\_ Street City, State Zip

Contact Information:

( ) ( )  
Home Telephone Mobile Email

Social Security Number: \_\_\_\_\_ Driver's License Number: \_\_\_\_\_

*How did you learn about our company?*

**POSITION SOUGHT:** \_\_\_\_\_ Available Start Date: \_\_\_\_\_

Desired Pay Range: \_\_\_\_\_ Are you currently employed? \_\_\_\_\_  
By Hour or Salary

How many hours a week can you work? \_\_\_\_\_

Employment desires:  Full-time only  Part-time only  Full or Part-time

**EDUCATION**

	Name and Location	Graduate? – Degree?	Major/Subjects of Study
High School			
College or University			
Specialized Training, Trade School, etc...			
Other Education			

If hired, can you show proof of age or provide a permit to work?  No  Yes

Have you ever been convicted of a crime:  No  Yes (if yes, explain) \_\_\_\_\_

# Privacy Please



## PREVIOUS EXPERIENCE

Please list beginning from most recent

Dates Employed	Company Name	Location	Role/Title

Job notes, tasks performed and reason for leaving:

---



---

Dates Employed	Company Name	Location	Role/Title

Job notes, tasks performed and reason for leaving:

---



---

Dates Employed	Company Name	Location	Role/Title

Job notes, tasks performed and reason for leaving:

---



---

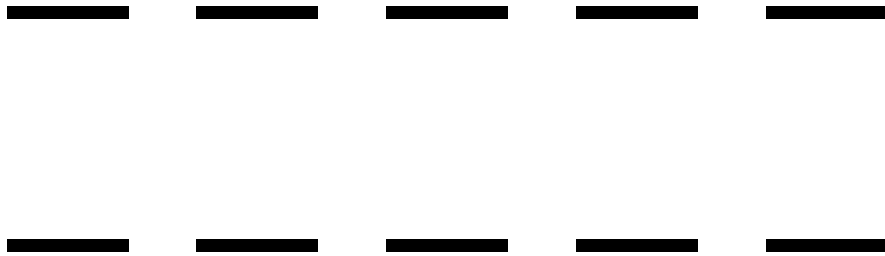
## REFERENCES

Please list references other than relatives and previous employers:

Name _____	Name _____
Address _____	Address _____
City, State, Zip _____	City, State, Zip _____
Telephone (____) _____	Telephone (____) _____
How do you know this person? _____	How do you know this person? _____

Your Signature \_\_\_\_\_

Place a



in your  
credit file.

*Answer: p. 20 of leader's guide*

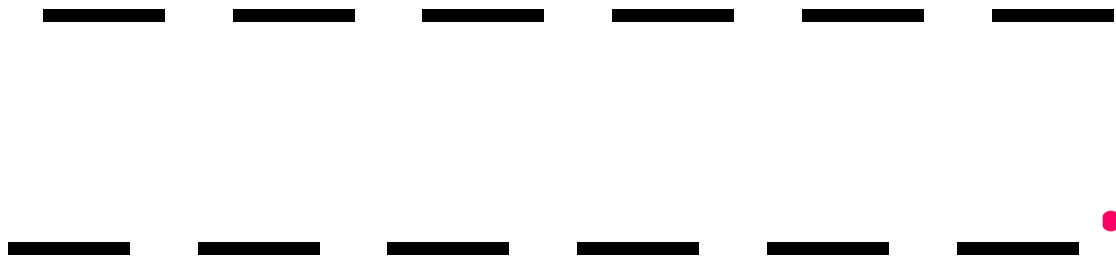


---

Privacy Please



Get a free  
copy of your



*Answer: p. 20 of leader's guide*

-----

-----

that have  
been used by  
identity  
thieves.

*Answer: p. 20 of leader's guide*

Complete an  
on-line  
complaint  
form with the

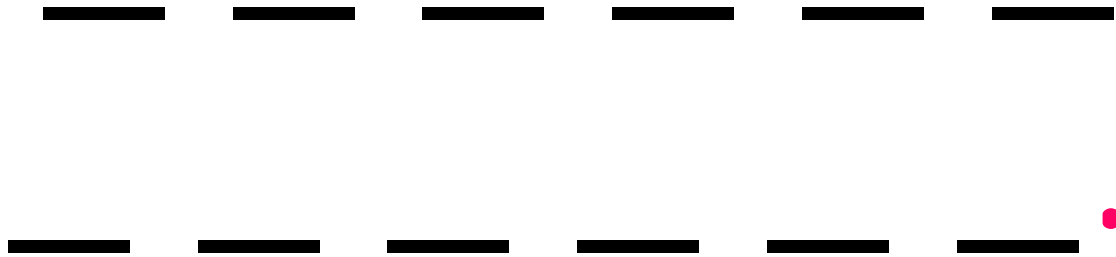
\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_.

*Answer: p. 20 of leader's guide*

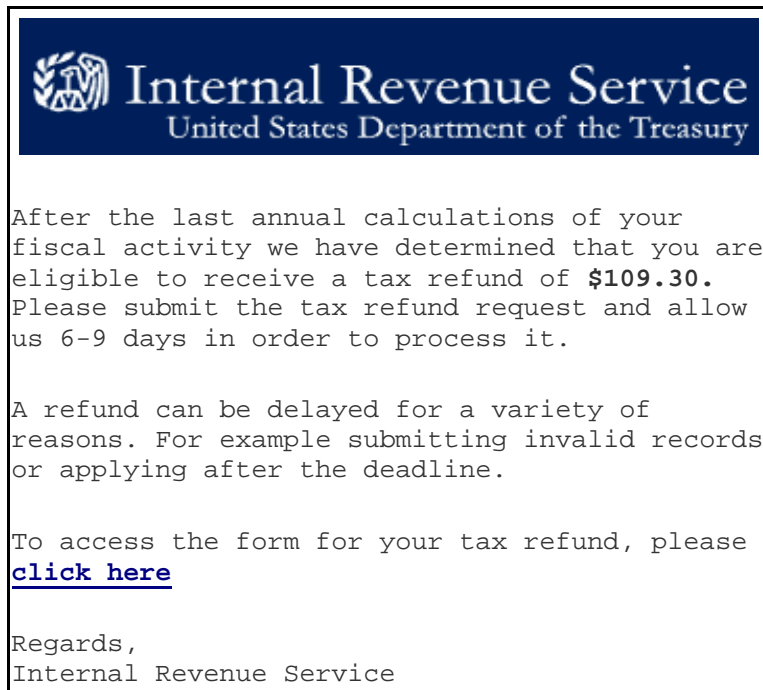
File a



*Answer: p. 20 of leader's guide*

---

## Privacy Please



© Copyright 2007, Internal Revenue Service U.S.A..

### Read through the phishing e-mail above and then answer these questions:

What gimmick are they using to grab your attention? \_\_\_\_\_  
\_\_\_\_\_

Why would someone pay attention to this e-mail? \_\_\_\_\_  
\_\_\_\_\_

What makes you suspect that this is a phishing e-mail? \_\_\_\_\_  
\_\_\_\_\_

Is this the usual way this company/agency communicates with customers? \_\_\_\_\_  
Why do you think so? \_\_\_\_\_

What should you do if you receive an e-mail like this? \_\_\_\_\_  
\_\_\_\_\_



# Privacy Please



Dear eShop customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information. This might be due to either of the following reasons:

1. A recent change in your personal information (i.e., change of address).
2. Submitting invalid information during the initial sign up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please update and verify your information by clicking the link below:

<https://arribada.eshop.com/saw-cgi/eShopISAPI.d11?PlaceCCInfo>

If your account information is not updated within **48 hours** then your ability to sell or bid on eShop will become restricted.

Thank you ,  
The eShop Billing Department

Copyright © 1995-2004 eShop Inc. All Rights Reserved.  
Designated trademarks and brands are the property of their respective owners.  
Use of this Website constitutes acceptance of the eBay

## Read through the pharming e-mail above and then answer these questions:

What gimmick are they using to grab your attention? \_\_\_\_\_

\_\_\_\_\_

Why would someone pay attention to this e-mail? \_\_\_\_\_

\_\_\_\_\_

What makes you suspect that this is a pharming e-mail? \_\_\_\_\_

\_\_\_\_\_

Is this the usual way this company/agency communicates with customers? \_\_\_\_\_

Why do you think so? \_\_\_\_\_

What should you do if you receive an e-mail like this? \_\_\_\_\_

\_\_\_\_\_

# Privacy Please



Dear **Washington Bank** Customer,

We recently reviewed your account, and suspect that your **Washington Bank Internet Banking** account may have been accessed by an unauthorized third party. Protecting the security of your account and of the **Washington Bank** network is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, please take the following steps to ensure that your account has not been compromised:

1. Login to your **Washington Bank Internet Banking** account. If you are not enrolled for Internet Banking, you will have to use your Social Security Number as both your Personal ID and Password and fill in all the required information, including your name and account number.
2. Review your recent account history for any unauthorized withdrawals or deposits, and check your account profile to make sure not changes have been made. If any unauthorized activity has taken place on your account, report this to **Washington Bank** staff immediately.

To get started, please click on the link below:

<https://login.personal.wab.com/logon/logon.asp?dd=1>

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire **Washington Bank** system. Thank you for your prompt attention to this matter.

Sincerely,  
The **Washington Bank** Team

Please do not respond to this e-mail. Mail sent to this address cannot be answered. For Assistance, log in to your **Washington Bank** account and choose the "Help" link in the header of any page.

## Read through the pharming e-mail above and then answer these questions:

What gimmick are they using to grab your attention? \_\_\_\_\_

\_\_\_\_\_

Why would someone pay attention to this e-mail? \_\_\_\_\_

\_\_\_\_\_

What makes you suspect that this is a pharming e-mail? \_\_\_\_\_

\_\_\_\_\_

Is this the usual way this company/agency communicates with customers? \_\_\_\_\_

Why do you think so? \_\_\_\_\_

What should you do if you receive an e-mail like this? \_\_\_\_\_



## Privacy Please

Hello,  
this is an update email to inform you about your mortgage/loan  
approval.

Eugenio Brunson called from Capital First Corporation  
yesterday to update your situation.

Our company will approve you for 1.45% but we need some  
information.

Please fill this form:

<http://nssm.ecadhfja.info/?JqLwfxdehNQ..1JATXfrfEPUI>

We will take care of the rest.

Thanks for your time  
Mauro

**Read through the pharming e-mail above and then answer these questions:**

What gimmick are they using to grab your attention? \_\_\_\_\_  
\_\_\_\_\_

Why would someone pay attention to this e-mail? \_\_\_\_\_  
\_\_\_\_\_

What makes you suspect that this is a pharming e-mail? \_\_\_\_\_  
\_\_\_\_\_

Is this the usual way this company/agency communicates with customers? \_\_\_\_\_  
Why do you think so? \_\_\_\_\_

What should you do if you receive an e-mail like this? \_\_\_\_\_  
\_\_\_\_\_



# Privacy Please



Dear Hummington Customer,

This email is to inform you, that we had to block your Hummington Bank account access because we have been notified that your account may have been compromised by outside parties. Our terms and conditions you agreed to state that your account must always be under your control or those you designate at all times. We have noticed some unusual activity related to your account that indicates that other parties may have access and or control of your information in your account. These parties have in the past been involved with money laundering, illegal drugs, terrorism and various Federal Title 18 violations.

**Please follow this link to complete your security verification and unlock your VISTA® check card :** <https://onlinebanking.hummington.com/security/login.jsp>

Please be aware that until we can verify your identity no further access to your account will be allowed and we will have no other liability for your account or any transactions that may have occurred as a result of your failure to reactivate your account as instructed above.

Thank you for your time and consideration in this matter .

Sincerely,  
Hummington Bank Accounts Department.

Note: Requests for information will be initiated by our Hummington Bank Business Development Group, this process cannot be externally expedited through Customer Support

## Read through the pharming e-mail above and then answer these questions:

What gimmick are they using to grab your attention? \_\_\_\_\_

\_\_\_\_\_

Why would someone pay attention to this e-mail? \_\_\_\_\_

\_\_\_\_\_

What makes you suspect that this is a pharming e-mail? \_\_\_\_\_

\_\_\_\_\_

Is this the usual way this company/agency communicates with customers? \_\_\_\_\_

Why do you think so? \_\_\_\_\_

\_\_\_\_\_

What should you do if you receive an e-mail like this? \_\_\_\_\_

\_\_\_\_\_

## Case Study: Setting up a Blog

Lee is creating a blog to meet friends and to increase his social network. He stops by the library after school to sign up for a FaceSpace account. When filling out his online profile, Lee:

- Uses the username, “Cool L” instead of his full name
- Creates a password and writes it down on the front of his biology notebook
- Fills out his profile, listing his favorite music, movies, television shows, and hobbies
- Decides to skip filling in which school he attends

When reviewing the settings of his account, Lee:

- Checks off the box to keep his complete profile private instead of viewable to the public
- Does not click on the setting to keep his e-mail restricted to people on his contact list. Anyone searching users on the site can send him an e-mail.
- Does not check off the box to review and approve comments before they are posted on his site for everyone to view

As Lee looks up at the clock in the lab, he realizes that he’s running late for his afternoon softball practice. He closes the browser instead of logging out completely and leaves the computer lab in a hurry.

**1. List (or highlight/underline with a marker, pen, or pencil) the things that Lee did to reduce the risk of identity theft.**

**2. List (or highlight/underline with a different color marker, pen, or pencil) what else Lee could do to better to reduce risks of identity theft.**

---

## Privacy Please



---

### Case Study: Applying for a job

Kesha is meeting her friends at the mall and sees a “help wanted” sign in her favorite clothing store. She fills out a job application for a sales clerk position and gives the following information:

- Name, address, phone number
- At the question “Are you over 18? Yes or No,” she circles “No” and writes in “16”
- Cell phone number
- Driver’s license number
- Leaves Social Security number section blank
- Hours of availability
- References

Kesha was supposed to meet her friends five minutes ago. She signs the application without reading the fine print at the bottom and hands the application to the sales clerk at the register.

**1. List (or highlight/underline with a marker, pen, or pencil) the things Kesha did to reduce the risk of identity theft.**

**2. List (or highlight/underline with a different color marker, pen, or pencil) what else Kesha could do better to reduce her risk of identity theft.**

## Privacy Policies for Websites

Read, “How to Read a Privacy Policy” at: [http://www.oispp.ca.gov/consumer\\_privacy/consumer/documents/pdf/cis6english.pdf](http://www.oispp.ca.gov/consumer_privacy/consumer/documents/pdf/cis6english.pdf)

**1. What information does the website collect from you?** *(check all that apply)*

- Email address
- Driver’s license number
- Citizenship
- Financial information (i.e., credit card numbers, bank account numbers, income)
- Medical information (i.e., health plan, diseases or physical conditions, prescription drugs)
- Social Security number
- Password
- Date of birth

**2. How is the information collected?**

**3. Why is the information collected?**

*(Pay attention if the business or website asks for information not related to why you are using the website. Find out why and how the unrelated information requested will be used. Look for a way to opt out of or say no to giving the extra information.)*

**4. How does the website use information collected from you?** *(check all that apply)*

- To send you emails
- To sell personal information to third parties
- To sell information to other companies and individuals in order to communicate with you by email
- Information is necessary for legal requirements such as a law, regulation, search warrant, subpoena or court order or to prevent a crime
- With your permission, to receive offers and promotions from partner companies
- To disclose or transfer your information to a third party that buys all or a portion of that business

**5. How does the website protect the information collected?**

**6. How does the website allow you to access, correct, or delete your personal information?**

**7. For questions or concerns, how would you contact the website about their privacy policy?**

---

## Privacy Please



---

## Warning Signs of Possible Identity Theft

1. **In your group, do an online search for a new or common identify theft scam. Visit the FBI <http://www.fbi.gov/> and FTC's <http://www.ftc.gov/> websites to learn about these scams.**
2. **Select one scam that is very devastating to the victim and develop and perform a 3–5 minute skit about the scam**
3. **Include in your skit the following:**

**Name & description of the scam:**

**How does the scam affect the victim:**

**What are the warning signs:**

**How to avoid or stop the scam:**

**1. List (or highlight/underline with a color marker, pen, or pencil) the things that Lee did to reduce the risk of identity theft.**

- Uses a username instead of making his full name public
- Does not fill in which school he attends so that other people can not use his information for illegal purposes
- Made his personal profile private to friends and contacts instead of searchable by the public

**2. List (or highlight/underline with a different color marker, pen, or pencil) what else Lee could do to better to reduce risks of identity theft.**

- Keep his e-mail restricted to people on his contact list. Anyone searching users online can send him an e-mail
- Check off the setting that allows him to approve comments from others before they are posted to the public. This can prevent people from posting malicious information about his identity
- Memorize his password or keep it in a safe place, so it is not accessible by others
- Clear the history and cache on the computer before leaving the computer lab
- Make sure to log off completely instead of just closing the browser

Another option to suggest to teens:

- Make sure the computer he uses is updated with current anti-virus protection, anti-spyware software, and a firewall.

---

## Privacy Please



---

**1. List (or highlight/underline with a color marker, pen, or pencil) the things that Kesha did to reduce the risk of identity theft.**

- Kesha did not write down her Social Security number.

**2. List (or highlight/underline with a different color marker, pen, or pencil) what else Kesha could do to better to reduce her risk of identity theft.**

- Do not include age on application. The application did not ask for her age and in some places it is against the law to ask an applicant's age.
- Did not read the fine print before signing. Many times the application states how the information collected on the application will be used, protected or shared. Kesha does not know how the information she has provided will be used.

Other options to suggest to teens:

- Leave her Social Security card in a safe place. Kesha should not carry it in her wallet. She should bring it with her only on the days she will need it.
- To keep her information private, Kesha should only give her application to a manager, if possible.