Money TALKS

Should I Be Listening?

Privacy, Please!

IDENTITY THEFT

How Thieves Work

AND NOW THE NIGHTMARE BEGINS

Keep It Safe!

IF YOU'RE A VICTIM

You've probably heard people talking about identity theft. Maybe it's even happened to you or to someone you know. But what exactly is identity theft?

Well, it's when someone steals your personal info and then uses it to get a credit card, rent an apartment, get a job, or to commit a crime. Not only are they pretending to be you, these thieves also leave you responsible to pay for their fun and the bills they run up.

This means that even though you didn't do anything wrong, you may still suffer the consequences of their actions. These consequences can mean paying for stuff you didn't buy, being denied school and car loans, not getting a job, or even being arrested! At the very least, you will be stressed out and inconvenienced while trying to prove your innocence to a credit card company. At the worst, you could spend years trying to repair your credit record, job history, and reputation.

UNIVERSITY of CALIFORNIA
Agriculture & Natural Resources
Publication 8405

IDENTITY THEFT

As one of the fastest growing crimes in the United States, identity theft affects 9 million Americans annually, according to the FTC. Altogether, identity theft victims will lose more than $5 billion dollars this year alone. Being a teenager doesn't mean you're safe. In fact, it means that you are at a greater risk. Since most teens don't have a credit record, thieves can open brand new accounts in your name and you won't even know it. If this happens to you, you may not find out for years until you try to get a loan. Because you are just starting your credit history, your whole financial future is at risk. And, if you don't have a driver's license, a thief could use your Social Security number to apply for one, and you'll only find out when you apply for a driver's license and are denied.

How High Is My Risk?

This quiz will help you find out just how much you are at risk for identity theft.

☐ Never ☐ Sometimes ☐ Always 1. How often do you throw away or recycle papers that have your personal information on them, like cash register receipts, pre-approved credit card offers, or your cell phone bill?

☐ Never ☐ Sometimes ☐ Always 2. How often do you use your full name on your online profiles, so that your friends can find you?

☐ Never ☐ Sometimes ☐ Always 3. How often do you finish using someone else's computer by just closing down the browser rather than logging out of your email, bank, or social networking accounts?

☐ Yes ☐ No ☐ Not Applicable 4. I check my debit card account activity at least once a week to make sure no one has used my account illegally.

☐ Yes ☐ No ☐ Not Applicable 5. I have given out my Social Security number on a health form, job application, or to a sports team official without asking why it was needed.

☐ Yes ☐ No ☐ Not Applicable 6. I take my credit card, debit card, or checkbook with me every time I go out, just in case.

☐ Yes ☐ No ☐ Not Applicable 7. I've shared passwords and account numbers with a few people who are really close to me because I know I can trust them.

☐ Yes ☐ No ☐ Not Applicable 8. I use file sharing programs to get new music and movies for free.

Scoring key on page 3

CONFIDENTIAL

Scoring KEY

Question 1: Never = 1 point; Sometimes = 2 points; Always = 3 points
Throwing away or recycling private information isn't enough. Thieves often look through trash to find information that will help them steal your identity. Instead, shred documents that contain personal information with a crosscut shredder.

Question 2: Never = 1 point; Sometimes = 2 points; Always = 3 points
Including information like your full name and date of birth on social networking sites (or any site for that matter) puts you at greater risk for identity theft. Instead, use a nickname and let your friends know what you've chosen.

Question 3: Never = 1 point; Sometimes = 2 points; Always = 3 points
If you just close out of a browser, you are not doing enough to protect yourself. Many sites keep you logged on until you log out. So the next person who uses the computer could access your private accounts. While your best bet is to access private information at your own computer, you should manually log off all sites you enter and delete the browser's temporary files before you leave someone else's computer.

Question 4: Yes = 1 point; No = 3 points; N/A=1 point
Watching your account history closely will let you know right away if someone has stolen your banking information. The sooner you catch it, the less it will cost you. If you catch it within two days and notify your bank, then you will only have to pay up to $50.00. If you notify within 2-60 days, you can be charged up to $500. And if you don't notify until after 60 days, you could be held responsible for the entire amount the thief spends, which could be thousands of dollars.

Question 5: Yes = 3 points; No = 1 point; N/A=1 point
Your Social Security number can be used by thieves to open credit accounts, get a driver's license, and even to get a job. There are only a few cases when your Social Security number is lawfully needed. So before giving it out ask: Why it is being requested? What will be done with it? How it will be protected? For more information, read "A Note About Your Social Security Number" on page 6.

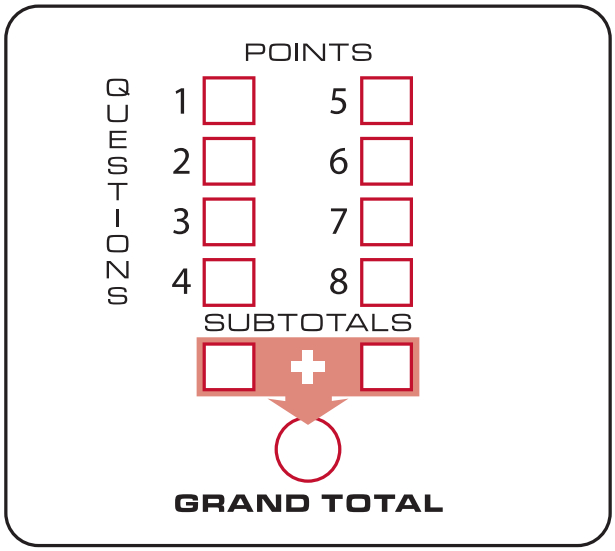
Question 6: Yes = 3 points; No = 1 point; N/A=1 point
Carrying your credit card, debit card, and checkbook around when you don't need them increases your chances of having them lost or stolen. If you're going out to a movie or dinner take only the amount of money you plan to spend. Not only will this keep your bank and credit card accounts safe, it may help you spend less money, too.

Question 7: Yes = 3 points; No = 1 point; N/A=1 point
Unfortunately, thieves who steal teenagers' identities are often people the teenagers know, even trusted family members. So, keep your passwords and account information private.

Question 8: Yes = 3 points; No = 1 point; N/A=1 point
While file sharing programs may seem like a cheap way to get stuff you want, they also give other users access to your computer and your files. Even if you have set up "to share" folders, users may still be able to get to your pictures, your bank statements, your passwords, everything. When this happens, file sharing programs can end up costing you a lot of money and time.

Your Score

Enter your score for each of the questions in the boxes below. Subtotal both columns. Add the subtotals together to get your grand total.



What Does Your Grand Total Mean?

8 - 13 points: Your risk of identity theft seems low, but you can never be too careful. Read on to see if you can find a few new ways to keep your identity safe.

14 - 19 points: Your risk of identity theft is moderate. This information can help you find ways to reduce your risk even more.

20 - 24 points: Your risk of identity theft is high, but it's not too late to start protecting yourself. The information in this quiz gives some good ideas for changes you can make to protect yourself. Read the rest of this guide for more information on how to protect your identity.

How Thieves Work

Thieves basically have two objectives. First, they want to get private information. Second, they want to use this information for their own benefit. How do they get access to information that is supposed to be private? They steal mail or credit cards and pick through trash. Read on to find out more about the many ways a thief can steal your personal information.

Skimming: This may be the most frequently used method of credit card fraud. Basically, it's when you give your credit card to a waiter, cashier, or doctor's office receptionist and they copy your account information. Thieves may also place a card reader in the card slider at an ATM machine. Your account information is recorded when you get money out of your account. Protect yourself by checking your account activity often.

Dumpster Diving: This is exactly what it sounds like. Thieves go "diving" (searching) through dumpsters, trash cans, recycling bins, and even trash heaps at the dump. All they need to find is one pre-approved credit card notice and they can open a credit card account in your name. But often times they will find much more. Shred all papers with personal information on them.

Computer Spyware: Spyware software can be downloaded onto your computer when you visit web sites or take your computer in for repairs. This software allows thieves to record your website history and everything you type, including account numbers and passwords. You can protect yourself by installing virus detection or anti-spyware software onto your computer and keeping it up to date.

Account Redirection: Thieves can go to the post office and fill out a change of address form to have your mail sent directly to their address. Or, they can call your financial institution and tell them that you have moved. Banks and credit unions will often send out letters to both addresses, so keep an eye out for this sort of mail. If you haven't moved, but you get a letter from your bank saying your address has been changed, call your bank ASAP—as soon as possible!

Continued on page 5

How Thieves Work (cont.)

Phishing: You've probably gotten a phishing email before. These emails seem like official messages from a bank or online store asking you to update your account information; but when you do, the information goes directly to the thief. Phishing can also happen over the phone, as a thief pretends to be a bank officer calling to discuss your account. If you think the email or call is valid, always call them back using a phone number you know you can trust, like the phone number on the back of your credit card. Whoever answers the phone will be able to connect you to the right department.

Pharming: Similar to phishing, pharming attempts to trick you out of your account or login information. Thieves create fake websites designed to look like a bank or online store and then buy domain names similar to the real web addresses. So when you accidentally type in the wrong web address, you end up at the fake site. When you log in, the thieves get your username and password. If you need to login to an account, do it directly through the company's website, not through an email link.

Wireless Hacking: If you use a wireless internet connection for your computer or cell phone, you could be hacked. Thieves look for unsecure connections and then tap into your information. Often times the thief will be sitting at the coffee table next to you or sitting in a car in the parking lot. Your best bet is to simply avoid accessing personal information if you are using an unsecured connection.

Stealing: By grabbing your wallet or purse, a thief can get access to a ton of information very quickly. These thieves often have an entire network set up to handle the contents of your purse or wallet, so that within minutes your credit card can be used or your bank account emptied. Or a thief can steal your incoming and outgoing mail from your home mailbox, which can provide instant access to your account information and pre-approved credit offers. Call your bank and other important institutions immediately if you suspect your information has been stolen. Never carry your Social Security card or number in your wallet or purse. Keep your card in a secure place and take it out when it is needed, such as when you are hired for a new job. Keeping a list at home of what is in your wallet or purse will help you know which companies to call if your information is stolen.

Shoulder Surfing: By watching you punch in your calling card number or listening to you give a friend your address, a thief can get information directly from you. Look around to make sure no one is listening before you talk about personal information. Or better yet, just don't share your personal information in public.

And now the Nightmare Begins

Remember: Always log off open websites.

Once your information has been stolen, the thief can sell it to someone else or use your name to:

- ☐ Open a credit line or get a loan
- ☐ Start phone service
- ☐ Start a utility service
- ☐ Rack up charges on your credit card
- ☐ Get a driver's license
- ☐ Get health care
- ☐ Receive government benefits
- ☐ Rent an apartment
- ☐ Get a job
- ☐ Empty your bank accounts
- ☐ Write checks from your account
- ☐ Avoid a driving ticket or other criminal charge

A Note About Your Social Security Number

You might be surprised how many people will ask for your Social Security number: schools, banks, potential employers, doctor's offices, rental applications, utility accounts, etc. When someone requests your Social Security number:

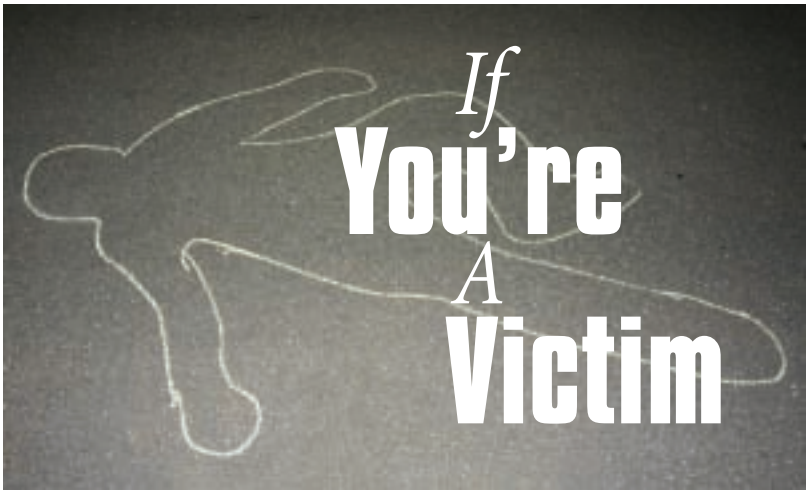
- ask why they want it
- how it will be used
- how it will be protected
- what happens if you don't give it to them

While employers and financial institutions are required by law to use your Social Security number, many times you'll be able to just leave that line blank. On most job applications, instead of giving your Social Security number, write in "available upon hire."

Keep It **Safe!**

19 Easy Ways to Protect Your Identity

1) Use passwords on your laptop, cell phone, and PDA.
2) Use passwords that mix letters, numbers, and symbols (if allowed).
3) Keep passwords secret.
4) Shred loan and credit card applications you get in the mail.
5) Guard personal numbers, like phone numbers, address, bank account, Social Security, date of birth, student ID, etc., even from trusted friends or relatives who don't need to know this information.
6) Use a crosscut shredder to destroy documents with personal numbers.
7) Regularly check your bank statements for unauthorized charges.
8) Don't write your bank account number on checks being deposited or cashed.
9) Use firewall, antivirus and anti-spyware programs on your computer.
10) Don't put personal information into your blog or on social networking sites.
11) Don't store personal information on a computer you share with someone else.
12) Wipe out your hard drive before you give away an old computer.
13) Check out website privacy policies to find out if your information may be shared.
14) Keep your credit or debit card in sight.
15) Don't give out personal information or passwords over the phone when you're in a public place.
16) Never give out your account numbers to a telemarketer who calls you (unless you have requested they contact you).
17) Don't use your cell phone to give out private information such as credit card numbers.
18) Don't be intimidated if a coach, teacher, youth group leader or other trusted adult asks for private information like your drivers' license, Social Security or credit card number. Don't give them the information. Refer them to a parent or guardian.
19) Starting at age 18, request and review free copies of your credit reports. Get your free reports from www.annualcreditreport.com

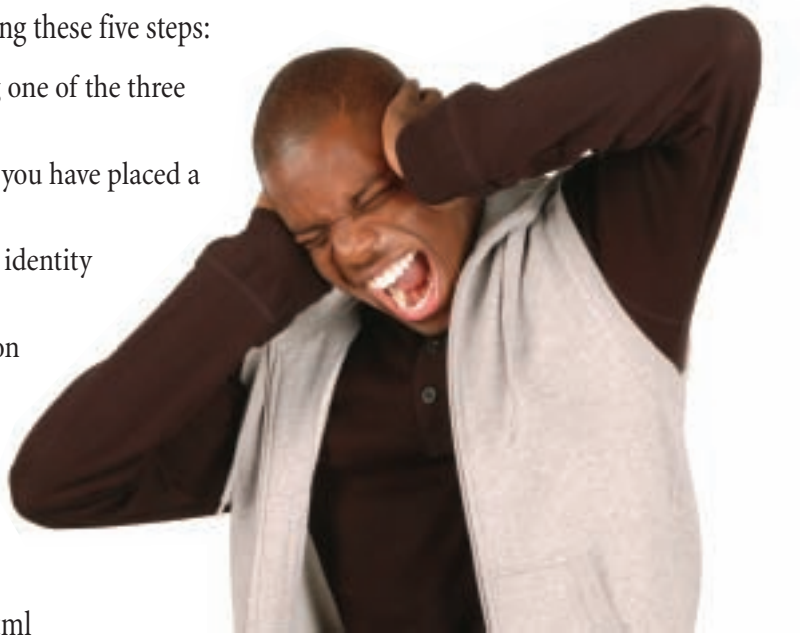


Did You Know?

- 15% of all ID theft cases are committed by a close friend or a family member of the victim.
- 29% of identity theft victims are between the ages of 18-29.
- Identity theft victims spend an average of 330 hours over 4-12 months repairing their records.

If your identity is stolen, take action immediately to reduce the damage done to your credit history or further loss of money from your bank accounts. Ask a trusted adult or your financial institution for help. Start by taking these five steps:

1. Place a fraud alert on your credit file by calling one of the three major credit reporting agencies.
2. Get a free credit report. You're entitled because you have placed a fraud alert on your file.
3. Close your accounts that have been affected by identity theft.
4. File a report with the Federal Trade Commission (FTC) at www.ftc.gov/idtheft
5. File a police report. Provide them with a copy of your completed FTC complaint form.



You can also visit these sites for step-by-step information on how to respond:

http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html

http://www.justice.gov/criminal/fraud/websites/idtheft.html

Money Talks…Should I Be Listening? Is a series of teen guides designed for teenagers. The topics and subject matter content are based on the results of a survey completed by teens. The goals of these teen 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 can be addressed to: Consumer Economics Department, University of California Cooperative Extension (UCCE), 135 Building C, Highlander Hall, Riverside, CA 92521. Author: Katherine Wassenberg, freelance writer. Development Team: Shirley Peterson, Karen Varcoe, Patti Wooten Swanson, Keith Nathaniel, Margaret Johns, Charles Go, Brenda Roche and the UCCE Money Talks Workgroup; Graphic Designer: Kerry Decker, UC Riverside. 2009

UC PEER REVIEWED

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 8405