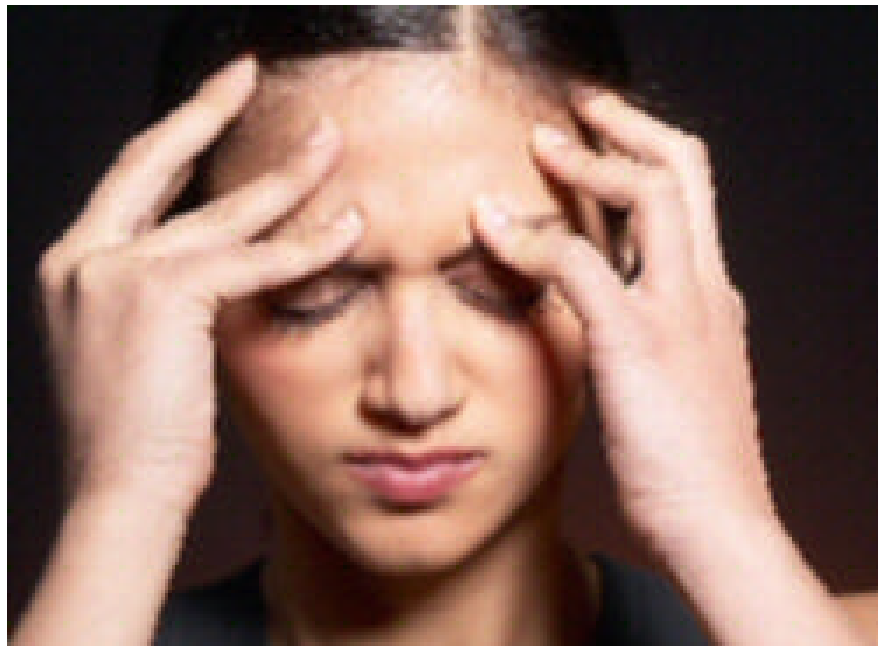


You may not sell this document nor change the links in it. Otherwise, you may distribute it freely.

# 80+ Ways to outwit identity thieves



and 17 ways to know when you're  
too late.

## **80+ ways to outwit ID thieves**

### **Your Social Security Number:**

1. In general, don't give out personal information. Just don't do it. Hardly anybody that you deal with in everyday situations has a legitimate need for more than your name, address, phone number and to see your picture ID.
2. Don't carry your Social Security card. Leave it at home in a secure place. Ditto for your credit and debit cards. Carry only the ones you intend to use that day.
3. If your state uses your Social Security number on your driver's license, ask them to use a substitute number. Ask your health insurance company to do the same if your policy number is the same as your SSN. And your student ID as well.
4. Almost every other situation where you will need to give your Social Security number will be a face-to-face encounter: a prospective landlord, a new employer, hospital or medical services, a new credit account or loan, etc. For utilities, insurance and other services that might be started by phone, make sure that YOU make the call and initiate the correspondence.
5. Unless you are attempting to initiate an open account with a company and they need your Social Security number to check your credit, ask why they need it. If you pay them by cash, check or credit card, they don't need your Social Security number.
6. Assume every email request for your personal information is fraudulent even if it appears to be from YOUR bank, credit card company, eBay, Amazon or other business you deal with online. Do not click on any links or paste them to your browser. Delete the email. Directly from your browser, go to their website and pull up your account. (If you don't have their internet address, typing their name into 'Google' will get it for you) Any problem they have with your account will show up there. If it isn't there, the email was a scam.
7. Find out what security procedures your workplace or business, doctor's offices or other institutions that collect your identifying information are using to secure it, who has access to it, how, and when it will be disposed of, and if they share your information with other agencies or institutions. Ask them to insure your information is kept confidential.
8. If you are using an accounting program on your personal computer, do not enter your complete social security or Fed ID numbers into it. Do it as \*\*\*\*\*xxxx. Just in case.

### **Your Bank account:**

9. Monitor your bank account statements closely. Question every item you don't recognize.
10. When using your debit card, shield the keypad from others as you enter your password.
11. Don't allow yourself to be distracted when using your debit card. Make sure you don't walk off and leave it.

12. Your bank sells your information to affiliates and third parties. Call them and opt-out.
13. Deposit your outgoing checks at the post office.
14. Do not have your Social Security number printed on your checks. Or write it there.
15. Do not write checks in ink or use an ink jet printer. Crooks can easily wash off, and replace, the payee and the amount. Use a laser printer or ball point pen.
16. When writing checks, don't leave blank spaces in front of the letters and numbers where crooks can raise the amount by entering more words and numbers.
17. Pick up boxes of new checks at the bank or have them sent to your box at the post office. Unless you have a locked and highly secured mailbox, rent a box at the post office or mail service to receive new checks and other financial information. If you will be on vacation call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold.
18. If you make your bank account accessible online to pay bills or receive payments, use a separate bank account just for that purpose. Keep a minimum of funds in the account and monitor it closely. **DO NOT KEEP YOUR MAJOR FUNDS IN THIS ACCOUNT.**
19. Just in case you have a malicious key logger program hiding in your computer, keep your log-in information in a .txt file. Copy and paste your password to login to your bank account. Log out completely and do not permit your browser to remember your username and password.
20. Do not store financial information on your laptop unless absolutely necessary. Laptops are routinely lost and/or stolen. If you must do so, use an extremely difficult password, do not activate automatic log-in features and log-off when your session is finished.
21. Don't abandon unused bank accounts. Actively close them and destroy (shred) unused checks and deposit slips.
22. Always shred old checks and bank statements before discarding them.
23. If you are using an accounting program on your personal computer, do not enter complete bank account numbers into the accounts. Do it as \*\*\*\*\*xxxx. Just in case.

### **Your Credit Cards**

24. Make it a practice never to give your credit card number to requests by email, over the phone or by mail. Instead call your bank or credit card company directly using their customer service numbers on their statements or on the back of their cards.
25. Don't allow yourself to be distracted when using your credit card. Make sure you don't walk off and leave it.
26. Notify your credit card company promptly of your change of address if you are moving.
27. When your credit card receipt has blank lines in it, like for tips etc., either fill them in or cross them out. Don't leave them blank.

28. Monitor your credit card statements closely. Question every item you don't recognize.

29. List each credit card, its account number, expiration date, and the telephone contact number shown on the back of the card. Keep list in a very safe place. Watch the expiration dates. If your new card doesn't arrive in a timely fashion, call the company to find out why. You may download and print a form we've created for this at:  
<http://www.aniota.com/recovery/cc-phone.pdf>

30. Your credit card companies sell your information to affiliates and third parties, flood your mail box with cash advance checks and offers for more up scale cards. And recently, they've even started signing cardholders up for third-party services. Call them and opt-out of their marketing programs.

31. Do not ever, ever cash an un-requested check. You'll be signing up for something. Shred all un-requested checks and applications you receive. Chop up expired cards and put the pieces in the garbage, not the trash.

32. If you have a death in the family, send a copy of the deceased's certificate of death to all credit accounts to close them.

33. If you are using an accounting program on your personal computer, do not enter complete credit card numbers into the accounts. Do it as \*\*\*\*\*xxxx. Just in case.

34. If you make your credit card accounts accessible online, keep your log-in information in a .txt file. Copy and paste to login to your account. (Just in case you have a malicious key logger program hiding in your computer.) Log out completely and do not permit your browser to remember your username and password.

35. Inquire of your credit card company if they offer "controlled payment" numbers or "virtual account" numbers, for online purchases. They are generally substitute numbers for online use instead of your real number.

### **Your Mail**

36. Deposit your outgoing checks at the post office, never ever in the mail box in front of your house. Consider getting a PO box to receive bills, checks and other sensitive information.

37. If you are not receiving your mail call the Postal Inspector General. You can locate the USPS district office nearest you by calling your local post office, checking the Blue Pages of your telephone directory, or visiting [www.usps.gov/websites/depart/inspect](http://www.usps.gov/websites/depart/inspect)

38. If you don't receive your bills, call creditors to find out why. In the case of credit cards, your \$50. limit of liability depends upon the creditor receiving your dispute letter within 60 days of when the bill was mailed even if an ID thief changed the address and you didn't receive the bill,

39. Offers of credit or investment advice in the mail alert thieves that you have good credit. To opt-out of receiving them, call: 1-888-5-OPTOUT (1-888-567-8688). They will ask for your Social Security number but, if you don't want to give it, will send you the paper work anyway.

40. Buy a cross cut shredder. (There are thieves out there who put the long strips together again) Good ones are available for less than \$100.00. Shred charge receipts, credit applications, insurance forms, physician and hospital statements, checks and bank statements, credit card offers.

41. Plan on mailing credit card payments at least a week before the due date to avoid late payment fees. Or consider paying them online.

42. Do not ever, ever cash an un-requested check you receive in the mail. You'll be signing up for something.

### **Your Telephone Service**

43. Be wary of "slamming" where your telephone service is switched from your current company to another one without your permission. Generally long-distance service but it can also happen with local or local-toll service. The fine print in contest entry forms, coupons, or other promotional materials might include an agreement to switch your phone service.

44. An imposter posing as a representative from your current telephone company may try to trick you by asking if you are satisfied with your service or if you're interested in a new calling plan or billing arrangement. A "yes" answer could be tape-recorded and used as proof that you agreed to switch. Just say "no" then call your phone company directly if you want to make a change.

45. Don't return calls to numbers on your pager or voice mail that you don't recognize. A slammer may use Automatic Number Identification to see the number you're dialing from and then process an unauthorized switch of service.

46. If you notice a new company name on your phone bill, call the number that's listed on that portion of the bill and ask for an explanation. If you've been slammed, inform the company that you didn't agree to use its service. Contact the company you originally had to switch back and reinstate in your old calling plan. Under federal law, you can switch back for free, and you don't have to pay for the first 30 days of service from the slammer. More than 30 days, you will pay your original company for that service from day 31 until the date you switch back. You will be charged your original company's rates, not the slammer's.

47. Put a "freeze" on your telephone service to forestall having your service switched to another company. You can lift it when you want to change.

### **Your Credit Report**

48. A credit reporting company can report most negative information about you for seven years, bankruptcy information for ten years, unpaid judgments for seven years or until the statute of limitations runs out, whichever is longer. There is no time limit on reporting: information about criminal convictions.

49. Place a fraud alert on your account: Residents of any state can put a fraud alert on their credit reports. Fraud alerts are supposed to alert you when someone applies for credit in your name and signals creditors to contact you for permission to issue credit in your name. Creditors, however, aren't required to abide by or even check the alert. Initial fraud

alerts last for 90 days and should be used when you suspect that you have been the victim of fraud. For an alert lasting for 5 to 7 years, you must provide evidence that you actually were the victim of identity theft. To set up a fraud alert on Equifax, call their Consumer Fraud Division at 1-888-766-0008. You will be presented with an automated voice response system that will allow you to input your personal information. Or write to Equifax Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374. Experian offers an online form to take your information. Contact TransUnion online or write them at P.O. Box 6790, Fullerton, CA 92834 Any one of these will forward your fraud alert to the other reporting agencies.

50. Members of the military away from their usual duty station may place an "active duty alert" on their credit report that is good for one year. Should you be deployed and businesses unable to contact you, you are allowed to use a personal representative to place or remove an alert. You'll also be removed from the credit reporting companies' marketing list for pre-screened credit card offers for two years unless you request reinstatement before then. To place such an alert, or have one removed, you should call one of the following three nationwide consumer reporting companies. The company will require you to provide appropriate proof of your identity.

Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com)

Experian: 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com)

TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com)

51. Place a freeze on your account: California residents, since 2003, have had the right to freeze their credit. This prohibits any credit from being issued in their names. Now, more states allow their residents the same rights: New Jersey, Louisiana, Texas, Vermont, Washington, Nevada, Connecticut, Illinois, Maine, North Carolina and Colorado. However, Texas, Vermont, Illinois and Washington limit this to victims of identity theft or a security breach.

With a credit freeze, no one can open any form of credit in your name. Lenders, insurers and even potential employers are not allowed to see your credit report. Because of this, most companies will not activate your account or issue credit or hire you. Should you want to get credit or allow potential employers to run a background check, the three credit bureaus will assign a PIN number for your use in lifting the freeze.

52. To freeze your credit report, contact each of the three credit reporting agencies. For most states, there is no cost if you are a victim of ID theft and have a police report. For residents of other states there may be a minimal charge to place the freeze and to lift it.

53. If adverse action is taken against you: Under federal law you're entitled to a free credit report if a company takes adverse action against you like denying your application for credit, insurance or employment, and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company that supplied the information about you. Under state law, consumers in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont already have free access to their credit reports

54. If you have a death in the family, mail copies of the certificate of death to all three agencies. In a few weeks check to see that there has been no fraudulent activity in the deceased's account.

55. Be aware that Services you pay to monitor your credit bureau accounts may be monitoring only one of them while charges against you may not migrate to all three agencies.

### **Your on-line Securities Accounts**

56. Before doing business with any investment-related firm or individual, be diligent in checking out their background and confirming whether they are legitimate. Check the SEC website for more information. <http://www.sec.gov/investor/pubs/onlinebrokerage.htm>

57. If you see a mistake on your statement or don't receive one, contact your brokerage firm immediately. Read your statements carefully as soon as they arrive to make sure that all transactions shown are ones that you actually made, and the ones that you thought you made appear as well. Be sure that your brokerage firm has current contact information for you.

58. Use extra caution with wireless connections which may not provide as much security as wired Internet connections. Actually, many networks in public areas like airports, hotels and restaurants reduce their security so it's easier for individuals to access and use these wireless networks. Unless you use a security token, accessing your online brokerage account through a wireless connection may not be worth the security risk.

59. A Security Token is a small number-generating device - a one-time pass-code that typically changes every 30 or 60 seconds. These unpredictable pass-codes frustrate identity thieves who use keystroke logging programs to obtain regular username and password information, cannot use them to obtain the security token pass-code. Inquire of your brokerage firm if you can use a security token or similar security device to protect your account.

60. In an article published October 26, 2006 in the RegisterUK, John Leyden reported that two US-based online brokerage houses attacked by a gang of identity thieves lost \$22 million. Using key loggers to snatch the account numbers of account holders, the thieves hijacked their accounts as well as creating new fraudulent accounts. The brokerage houses covered customers' losses. They have instituted extra security measures, mainly new anti-fraud technology, and their customers' use of two-factor authentication to remove the security risk posed by static login credentials

61. Consider keeping your login information in a .txt file where you can copy and paste it to access your account. Log out completely and do not permit your browser to remember your username and password.

### **Your Real Estate**

62. Go to the Assessors Office in your county (or to their website on-line) and look up your piece of real estate. You will need the legal description of the property (as shown on your deed and/or title) this is different than the street address) to make sure all the ownership and mortgage information is correct. If the ownership has been changed, or the mortgage holder is unknown to you, you should contact an attorney immediately. Generally when ID thieves take over someone else's real estate, the owners haven't a clue until the property has been sold, rented or foreclosed and it's far too late to prevent it.

63. Be aware that if you are selling your real estate and have listed it on one of the online websites, thieves can capture the address and the pictures from the net. They then adver-

tise the property for rent and either ask for a deposit for the keys to inspect the property or they get deposits from prospective renters who, in some cases, have even moved in without the owner ever knowing about it. Obviously, if you are not in a position to observe the property daily, you need to enlist the help of someone who is.

### **Your Tax Preparer**

64. Avoid preparers who claim they can obtain larger refunds than other preparers, who guarantee results or base fees on a percentage of the amount of the refund, who delegate your work to someone with less training or export it to workers in a foreign country. Unless you have a personal referral from several people who have used the preparer for years, you must use due diligence by:

65. Investigating whether the preparer has any questionable history with the Better Business Bureau, the state's board of accountancy for CPAs, the state's bar association for attorneys or the IRS Office of Professional Responsibility (OPR) for enrolled agents.

66. Checking the preparer's credentials. Is he or she affiliated with a professional organization? An Enrolled Agent, Certified Public Accountant (CPA) or Tax Attorney? Only attorneys, CPAs and enrolled agents can represent taxpayers before the IRS in all matters including audits, collection actions and appeals. Other return preparers may represent taxpayers only in audits regarding a return that they signed as a preparer.

67. Make sure the preparer has signed the form with their identifying number and filled in all the spaces. Make sure your identifying and financial information is correct. Don't sign a blank form, don't sign in pencil, and do get a copy.

### **Your e-mail and the Internet**

68. If at all possible use an email program other than MS Explorer. In any program that you DO use, set it to receive mail in .txt format. That will defeat any malware java scripts designed to contaminate your system.

69. Delete spam emails without opening them. Don't click on links in emails even if the email looks legitimate. Effective scams are designed to look legitimate. And don't open attachments unless you are sure you can trust the sender.

70. Beware of "phishing" where emails direct internet users to a fraudulent website to "fix" their accounts, and "pharming" where users, without their knowledge, are redirected from sites they frequently use to bogus look-alike sites where id thieves capture log-in names, passwords, and account numbers. "Pharming" is done by email attachments and one letter typos when typing in URL addresses. Make sure the website you arrive at is secure, that the http is followed with an "s" i.e. https.

### **At work**

71. Don't assume that your emails, your hard drive and your personal information is private and protected. Do assume that everything you write and everything in your files can appear on the internet, and the evening news, tomorrow! You can no longer assume that your employer, or your fellow employees, have your best interests at heart. Always use passwords on your files, but that is not completely reliable anymore, and encryption is not universally permitted.

72. As a general rule, do not bring your personal information to work. Human Resources

(Personnel) may HAVE to have it, but nobody else, even you! Anything you MUST have, keep it in your wallet or your purse (and keep your purse locked up) and remove it as soon as possible. If you write personal mail or personal checks, drop them in the US mail box out on the street.

73. If you are an independent contractor, a sole proprietor, use your Federal Identification Number instead of your Social Security Number. Also, give your Federal ID number, not your Social Security Number, to internet companies that will be paying you.

### **At Home**

74. A paper published by The Better Business Bureau Online reports that, when the victim can identify who stole their personal information, that "Almost half (47 percent) of all identity theft is perpetrated by friends, neighbors, in-home employees, family members or relatives."

75. Without being totally paranoid about it, keep your private data private. Lock it up in a desk drawer. Put your purse or wallet away, out of sight. Don't leave anything lying around for anyone to see and/or steal. And don't loan your credit or debit cards to anyone.

76. When you access the Internet you are at great risk of having your identity stolen. At one time or another, take it for granted, your own computer will be corrupted. Viruses, malware, spyware and Trojan horses infest emails, downloaded files, downloaded free-ware, shareware, software programs, and in downloaded pictures. They'll even seek out and hide in interactive programs you have on your computer. And, sometimes, a site you visit on the web is infected and then you've got it! Any log-ins and passwords, financial records, tax returns, birth date, and bank account, credit card and Social Security numbers that you have on your computer are there for the taking. To be really smart, put all your sensitive information on a floppy or CD and keep it off your hard drive altogether. It will still be handy when you need it.

77. If you use an accounting program to keep your accounting records, enter bank or credit card account numbers as \*\*\*\*\*xxxxx rather than complete numbers. As far as possible, keep your personal records and data on CD or floppy rather than on your hard drive. They will still be available when needed.

78. Keep patches for your operating system current. Use a firewall program that will block uninvited access to your computer. Without it, hackers can take over your computer and, without your knowledge, use it for any purpose they want. Use virus protection software and update it regularly. Update browsers with the latest version available. If submitting information over the internet, look for the "lock" icon on the browser's status bar to make sure your information is safe.

79. Use a "wipe" utility program to overwrite the entire hard drive before you dispose of your computer. Just deleting or reformatting the hard drive may not adequately get rid of your stored information. There are programs out there that can retrieve it.

### **Seniors**

80. If you are a senior, you have become a favorite target of fraudulent telemarketers, internet scammers, predatory lenders, and others pushing unbelievably good deals, wealth, money, lottery winnings, high returns on your investments, or some other benefit

you would not ordinarily receive. Once your name is on a "sucker list" it is sold to other scammers.

81. Fraudulent telemarketers are masters of psychological manipulation. In very short order, they find out which buttons to push that will make you "believe" in the scam and become a willing participant in your own financial destruction. Their tactics range from battering (agreeing with the scammer being the only way to end the verbal hammering),  
insidiousness (the scammer weasels his or her way into your life),  
seduction (making you feel accepted and loved),  
sympathy (to save (read that money) the scammer from loss or being fired), guilt (you owe them),  
threats (you'll lose all you might have gained in the future)  
to name only a few. Once they've got their hooks into you, it will be almost impossible to escape.

82. Stop it before it starts. HANG UP THE PHONE! Scammers hook you in by TALKING to you. They are powerless if you don't listen.

83. You can still be polite, considerate and kind by immediately interrupting the spiel and saying, "No, I don't think so. But thank you for calling." and immediately HANG UP THE PHONE! Do not, DO NOT wait for a response. I have never known of an instance where they called back, but if they do, HANG UP THE PHONE!

84. If the call appears to be so plausible, so legitimate, that you aren't immediately aware that it's an attempt to persuade you to give them personal information, subscribe, invest, buy, contribute, donate, etc., ask the caller to send you information in the mail. If they are legitimate, they'll be glad to do that. If not, HANG UP THE PHONE!

85. Practice paranoia. Offers that were entirely legitimate in the past are used by scammers today. Before you give your credit card information to anyone for anything, search the Internet for complaints about the program or the company. Check the online Better Business Bureau and even your state Attorney General's office. A few minutes of research can save you a load of money and hours and hours of grief.

86. Some credit card payments are sent to "cardmember services" rather than the actual credit card company. Now, fraudsters are calling on the phone in the name of "cardmember services" offering to reduce your interest. Sounds really legitimate until they get to "what is your card number?" If they were legitimate, they would know that! HANG UP THE PHONE!

## **17 Ways to tell if your identity has been stolen**

1. That you receive a notice or letter from the IRS indicating that more than one tax return was filed for you or that you received wages from an employer you didn't work for.

2. That you are failing to receive bills or other mail.

3. That you are receiving credit cards you didn't apply for.

4. That you are not allowed to open a new bank account.

5. That your credit cards are not being accepted.
6. That your checks are not being accepted.
7. That you are being denied credit, or being offered less favorable credit terms for no apparent reason.
8. That you are being denied rental housing, insurance or employment for no apparent reason.
9. That you are receiving bills for products or services you didn't buy.
10. That charges show up on your credit cards for products or services you didn't buy.
11. That you are being harassed for payment by collection agencies and/or lawyers for products or services you didn't buy.
12. That your bank or securities accounts show withdrawals you did not make or you are completely stripped of funds.
13. That your returned checks show different payees and larger amounts than you wrote them for.
14. That fraudulent checks cleared your account.
15. That utility, phone and tax bills show up for addresses that are not yours.
16. That you are arrested for a felony, misdemeanor or traffic violation that you did not commit.
- 17 Any unexpected change at all in your mortgage payments or real estate assessment and/or tax bills.

Copyright © [JHWhite](#) 2010



[Case Management Workbook for victims of ID theft and fraud](#)