

80 plus ways to protect yourself from 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.

Your Bank account:

8. Monitor your bank account statements closely. Question every item you don't recognize.
9. When using your debit card, shield the keypad from others as you enter your password.
10. Don't allow yourself to be distracted when using your debit card. Make sure you don't walk off and leave it.
11. Your bank sells your information to affiliates and third parties. Call them and opt-out.

12. Deposit your outgoing checks at the post office.
13. Do not have your Social Security number printed on your checks. Or write it there.
14. 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.
15. 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.
16. 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.
17. 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.**
18. 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.
19. Don't abandon unused bank accounts. Actively close them and destroy unused checks and deposit slips.

Your Credit Cards

20. 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.
21. Don't allow yourself to be distracted when using your credit card. Make sure you don't walk off and leave it.
22. Notify your credit card company promptly of your change of address if you are moving..
23. When your credit card receipt has a blank in it, like for tips etc., either fill them in or cross them out. Don't leave them blank.
24. Monitor your credit card statements closely. Question every item you don't recognize.
25. 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.

26. 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.

27. Shred all un-requested checks and applications you receive. Don't put them in the trash. Chop up expired cards and, if possible, put the pieces in the garbage, not the trash.

28. 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.

Your Mail

29. 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

30. 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,

31. Offers of credit 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.

32. 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.

33. 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 Telephone Service

34. 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.

35. 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.

36. 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.

37. 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.

38. 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

39. 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.

40. 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.

41. 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

Experian: 1-888-EXPERIAN (397-3742); www.experian.com

TransUnion: 1-800-680-7289; www.transunion.com

42. 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.

43. 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.

44. 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

45. 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.

Your on-line Securities Accounts

46. 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>

47. 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.

48. 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.

49. 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.

50. In an article published October 26, 2006 in the Register, 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

51. Log out completely and do not permit your browser to remember your username and password.

Your Real Estate

52. 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.

53. 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 advertise 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

54. 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:

55. 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.

56. 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.

57. 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.

Should you buy Identity Theft Protection and/or Insurance?

58. According to the editors of Consumer Reports magazine, the benefits are usually limited and "typically not worth the money." The National Association of Insurance Commissioners cautions consumers that insurance "cannot protect you from becoming a victim of identity theft and does not cover direct monetary losses incurred as a result of identity theft." It simply covers some of the expenses you will incur to deal with the problem, such as the costs of making phone calls and copies, mailing documents and possibly some legal bills. Also, since creditors typically insist upon dealing with the debtor/victim directly, a service cannot take this burden off your shoulders. The insurance cost will typically run from \$20 to \$100 per year with the deductible being from \$100 to \$250, with some as high as \$1000.

59. Before subscribing to any of the identity theft protection companies, LifeLock, Loud Siren and Trusted ID among them, go to the Consumer Reports Org. website at <http://www.consumerreports.org/> and search for "identity theft protection." You'll find several reviews of these companies and the services they actually provide.

60. American Express makes identity theft assistance available to cardholders for free. It provides round-the-clock telephone access to company representatives who will "help you determine if your identity has been stolen, navigate the recovery process, and protect yourself in the future." To speak with an American Express ID Theft Assistance representative, cardholders may call 1-800-297-7672.

Your e-mail and the Internet

61. As general rules, delete spam emails without opening them, don't buy anything offered in a spam email. 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.

62. In a White Paper entitled "The Top 5 On-Line Identity Theft Attacks," Amichal Schulman, Co-founder, CTO of Imperva, Inc. says: internet connected Web applications have played a central role in the growth of identity theft. They provide a convenient link between international crime organizations (often residing in Russia, Indonesia, and Nigeria) and vast inventories of world wide identity information. By exploiting vulnerabilities in ecommerce, banking, healthcare, and human resource applications, these criminal organizations have found that they can access back-end databases containing identity information. Then, the Internet provides them with a relatively anonymous medium for utilizing identity information. New accounts and credit instruments, cell phone accounts, bank accounts, credit cards, auto loans, and short-term bank loans can all be approved online without any requirement for physical proof-of-identity.

63. If you access the Internet, your computer may expose you to great risk of having your identity stolen. At one time or another, take it for granted, your own

computer will be corrupted by something. It happens by viruses and spyware sent by emails, by downloaded files, downloaded freeware, shareware and other programs, even in downloaded pictures. And, sometimes, a trusted site you visit has unknowingly hosted a virus or spyware program. And then you've got it! But you don't know it and 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.

64. 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 such as banks and credit card company to bogus look-alike sites where id thieves capture log-in names, passwords, 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.

65. AARP reports that consumer losses from Phishing are increasing but money recovered is going down. In 2004 there were \$137 million in losses, \$257 average per victim, with money recovered at 80%. In 2006, the losses were \$2.8 billion, an average per victim loss of \$1,244 and the money recovered only 54%. Another study reported by the Gartner Group shows that, on average, the amount of money lost to fraud rose from US \$1,408 in 2005 to US \$3,257 in 2006. The percentage of funds recovered dropped over the same one-year period from 85 percent in 2005 to just 61 percent in 2006.

At work

66. 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.

67. 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.

68. Don't leave anything visible in your car, mail, packages, etc. And always lock your car (even when you're in it).

69. 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.

Your online business

70. Be suspicious of orders with different "bill to" and "ship to" addresses, orders from free email services, orders larger than typical and requiring next day delivery, orders paid for by cashier's check or Western Union transfer, and those with international ship-to addresses. Make every effort to verify the buyer's identity and

that they did, in fact, place the order. Should you find yourself the victim of a scammer or credit card thief, notify your merchant credit card processor immediately.

Your Home

71. In a paper published by The Better Business Bureau Online at <http://www.bbbonline.org/IDtheft/safetyQuiz.asp> they report 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."

72. 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.

Your computer

73. If you use an accounting program to keep your accounting records, don't enter your bank or credit card account numbers unless absolutely necessary. As far as possible, keep your personal records and data on CD or floppy rather than on your hard drive. It will still be available when needed.

74. 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.

75. 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.

76. Be wary of freeware and shareware computer programs. Increasingly, these programs are including executable malware programs of one sort or another.

Seniors

77. Seniors have become a favorite target of fraudulent telemarketers, internet scammers, predatory lenders, and others pushing "deals" on them that promise wealth and other gains. Once a victim's name is on a "sucker list" it is sold to other scammers.

78. These criminals are masters of the psychological manipulation of seniors. In very short order, these manipulators find out which buttons to push that will make the victim "believe" in the scam and become a willing participant in his or her own financial destruction. Their tactics range from battering (to agree with the scammer being the only way to end the verbal hammering), insidious (the scammer weasels his or her way into the victim's life), seduction (making the victim feel accepted and

loved), sympathy (to save (read that money) the scammer from loss or being fired), guilt (the victim owes them), threats (the victim will lose all they would have gained in the future) to name only a few. Once they've got their hooks in the victim, it is almost impossible to escape.

79. The victim must ask for help. First, to determine if the scheme is a scam. And, if that is the case, to accept the fact that his or her belief in it was misplaced, that the scammer was not their friend and the promises were lies, and that the money already paid is irretrievably gone. And second, to help them salvage anything they have left. They need outside help to escape the scammers, who are not likely to give up easily, and their tactics of pressure and trickery that have been working for them so well. It's likely the conditioning the senior has been subjected to has rendered them unable to withstand it without help. The senior needs someone they've authorized to intercede between them and the scammer who will end the scammer's contact.

80. Toward that end, the senior should ask someone to help them that they have a history with, someone known for a long time and trusted absolutely, perhaps a family member or lawyer. If no one comes immediately to mind, they might consider asking their pastor or local Senior Center to recommend someone they know to be trustworthy. Still, ask for references and check them out carefully.

And finally

If you are considering making an online sale to or purchase from a company you have no prior dealings with or knowledge about, the Better Business Bureau Online makes checking these companies out simple and easy. Unfortunately, some of the state consumer protection agencies have information about these companies, but they won't tell you what it is! What?????????

Copyright © JHWhite 2008

JHWhite is the author of this article as well as the author and publisher of the CASE MANAGEMENT WORKBOOK for victims of ID theft and fraud" available on the website at: <http://www.aniota.com/~jwhite/wk-bk.html>