



# Identity *Theft*





**Don't Be a Victim!**

**By Darlene Greene**

**Identity theft has become one of the fastest growing crimes in the United States. Stealing identities requires thieves to learn all about you and your activities. They quickly learn which people may remain unaware for months that thieves victimized them. Identity thieves bank on victims being clueless - don't let them! As with most everything else in life, where your credit is concerned, no one else is looking out for you. You have to take all steps possible to protect yourself!**

## **How does identity theft happen?**

In many cases, theft results from a creditor allowing your personal data to be vulnerable. The following circumstances provide the most fertile ground for identity theft when a creditor...

-  inadvertently employs unscrupulous individuals who steal and sell information.
-  fails to properly destroy information.
-  loses the information somehow.
-  provides marketers or third parties (vendors, subcontractors) access to your information.

Other times, the theft results from an individual's lack of awareness. People dump pertinent personal data or "free offer"/"pre-approved" mailers in the trash without shredding them. They leave valuable information lying on their desks at work, on the seat of their cars, or carry it in a handbag or wallet where a thief can swipe it easily.

While the government offers some regulation of our personal data, existing law remains unclear and certainly not extensive enough for you to feel secure. You must create your own security and vigilantly protect your personal data.

# How can I reduce access to my personal data?

Don't carry more information than you need in your wallet or handbag. Carry one piece of identification and not more than one or two credit/debit cards. Don't carry your social security card, your passport (unless you are actually traveling), your insurance card (which usually has your social security number on it), your checkbook, or any other documentation with personal data on it unless you absolutely need these items.

When you must carry additional documentation or cards with you, keep them separate from your purse or wallet. If one is stolen, the thief won't get away with everything at once.

Reduce the amount of information that is easily accessible about you. Don't use your social security number on identification such as your driver's license. Don't print it on your personal checks or allow someone to write it on a check when verifying your identity.

Don't answer questions or surveys from telemarketers. Have your name removed from their call lists and from the credit bureaus' (Equifax, Experian, and Transunion) marketing lists. Put your phone number on the National "Do Not Call" list and "opt out" of the credit bureaus marketing lists: visit [www.donotcall.gov](http://www.donotcall.gov) (888-382-1222) and [www.optoutprescreen.com](http://www.optoutprescreen.com) (888-5OPTOUT). You also can get on the Do Not Call Registry Interaction with state registries: [www.ftc.gov/bcp/conline/edcams/donotcall/statelist.html](http://www.ftc.gov/bcp/conline/edcams/donotcall/statelist.html)

Have your name and address removed from the phone book and reverse directories.

Use a post office box or a commercial mailbox service. Never leave home for any extended period without having your mail and newspaper subscriptions put on hold.

When ordering checks, deposit slips and/or other supplies from your bank, pick them up at your local branch or have them sent to your post office box.

Do not leave mail in your mailbox for the postal courier to pick up or in open boxes at the reception desk of your office. At the very least, put them in a local drop box, but it's better to mail them in the boxes inside the post office.

Cancel all credit cards but the one credit card you can use anywhere. **DO NOT APPLY FOR STORE CARDS EVEN WHEN OFFERED A SAVINGS ON THAT DAY'S PURCHASE.**

Any company that sends you their privacy policy may be telling you within that form that they will allow "trusted" institutions access to your account information with them unless you call and/or write them specifically stating that you do not wish to be included on any lists or your information shared with any other institution. Read the notices that come from companies you do business with to be sure you're not agreeing to share your personal data inadvertently or by default.

Make photocopies of all important documents, photo id, credit cards, and insurance cards and keep it somewhere separate and safe. It will be much easier for the authorities to track thieves when notified of a problem with these copies in hand.

Take your credit card receipts with you. Put them in your wallet and/or purse. When you get home put them in an envelope or box and keep them for one year. At the end of the year, you can go through and shred those you don't need, give your tax advisor any that he/she needs to complete your tax return, and save the ones for any major purchases to ensure if there is a problem later you have proof of the sale. **NEVER** just throw them in the trash or leave them in the empty shopping bag.

# Pins and Passwords

Whenever possible in creating pins and passwords, use combinations of upper and lower case letters with numbers and a symbol. **DON'T USE ANY PERSONAL DATA SUCH AS BIRTHDAY, PART OF YOUR SOCIAL SECURITY NUMBER, ADDRESS, PHONE NUMBER, ETC.**

Once you've created them, memorize them. If you must keep a reference, keep it somewhere safe under lock and key. Don't keep it in your daily planner, wallet, or any other place where it could be accessed or stolen.

## Internet and Computer Safety

The internet is a wonderful tool and gives access to previously unimaginable amounts of information. That flow of information works both ways and unless you are careful, you can risk access to your computer unknowingly.

Avoid free offers, free downloads, free software and contest sites. Web services such as Webshots and Free Download sites install keystroke monitoring programs that transmit your data to crooks.

Regularly delete your temporary files, cookies, etc.

Update your virus definitions **EVERY DAY** or first thing **EVERY TIME** you start up your computer.

Install a firewall on your computer, especially if you use a high-speed internet service. Password protect personal or sensitive data files. Use 6-8 characters combining numbers, letters (upper and lower case) and a symbol.

When upgrading and/or disposing of old computer hardware, use appropriate software to "wipe" the hard drive clean of all data or physically remove and destroy the drive.

Chose carefully before entering personal information such as your telephone numbers or social security number online. If you are required to do so, read the privacy statement of the site thoroughly and make sure that your information is not shared with third parties or marketers. You also should check to make sure that such information is submitted via a secure link. To find out if the process is secure, look for a current security seal from Verisign or Thawite (if it is current, you will be able to click on it and receive a confirmation page at the provider's site). 128 bit security is common online and all reputable merchants will offer this grade of secure data transmission.

In Internet Explorer, a secure transaction is indicated several ways. One way is a browser alert, such as this:



You should also see a lock emblem in the lower right hand corner of your toolbar, like this (in some browsers this may also appear as a gold key):



Regularly check the major search engines such as Yahoo and Google for your name and associated variations. If you use quotation marks around your name, i.e. "Jane Smith" you'll get back the most accurate results. This will alert you as to how your name is being used online.



# When Preventative Measures Fail

If your personal data or property containing personal information is stolen, report it immediately to your local sheriff or police department, your creditors, the credit bureaus, your financial institutions and your employer. Keep copies and/or documentation of all reports, contact names and phone numbers. Close and/or transfer any vulnerable accounts to new ones. Be diligent in your record keeping of all activity following the theft, both yours and the thief's, if possible. Seek the assistance and advice of a qualified legal advisor. Identity thieves can be caught and your credit can be repaired. Being persistent and keeping good records will make the process swifter and easier.

Copyright © 2005 Protect Your Good Credit, All Rights Reserved  
Protect Your Good Credit; 11357 Nuckols Road PMB 129; Glen Allen, VA 23059  
Toll Free Phone: (800) 697-9873 Fax: (804) 377-9354

These materials do not constitute legal, compliance, financial, tax, accounting, or related advice. The end user of this information should therefore use the contents of this program and the materials as a general guideline and not as the ultimate source of current information and when appropriate the user should consult their own legal, accounting or other advisors. Any case studies, examples, illustrations cannot guarantee that the user will achieve similar results. In fact, your results may vary significantly and factors such as your market, personal effort and many other circumstances may and will cause results to vary.