

Stop, thief! That's my identity you're stealing!

Chet Braswell, PTH

Identity theft is one of the fastest-growing crimes in America. Federal officials and consumer groups estimate there are between 500,000 and 700,000 cases of identity theft each year. These crimes cost victims more than \$765 million annually. Last year, identity theft was the number-one consumer complaint to the Federal Trade Commission.

Unfortunately, the electronic age has helped the identity thief immensely.

What can I do to protect myself?

All that an identity thief needs to ruin your good name is your birth date, Social Security number and other identifying information such as your address and phone number. So, your protection strategy begins with the protection of these identifiers.

You should start by adopting a "need to know" approach to your personal information. Your credit card company or bank probably already has your mother's maiden name — or some other bit of information unique or private to you — for identification purposes. If you receive a phone call from someone claiming to represent your bank or credit card company requesting information that company should already have, be very suspicious. An identity thief may have targeted you.

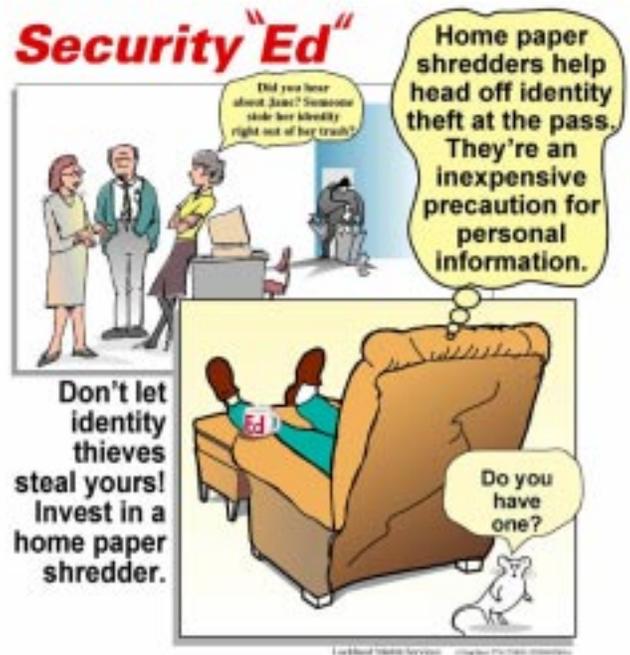
If someone calls and offers you a chance for a major prize, credit card or other valuable item and then asks for personal information, ask him or her to request the information in writing. If the person refuses to send the request in writing, you should terminate the call immediately. If the information is requested in writing, you can verify the authenticity of the request through the Better Business Bureau.

Thwart the dumpster divers — those who collect personal information on you by reviewing your trash. Shred sensitive matter such as pre-approved credit card applications, payroll check stubs, credit receipts and all monthly bill information. Security experts recommend using a shredder, and crosscut shredders are best. If strip shredding is used, insure that the strips cut across the text and do not allow lines of information to remain intact.

Do not carry sensitive information in your wallet. Minimize the number of credit cards you carry, and never carry your Social Security number with you.

When away from home for more than a couple of days, have your mail held at your local Post Office or have a trusted friend collect your mail daily.

Avoid the use of cordless and cellular phones when relaying personal or financial information.



Don't forget to send your ideas for Security Ed (the armchair know-it-all) to: Security Education, L4-09, or e-mail them to ^Security Education PHMC. If your idea is used, you will receive a credit line in the Hanford Reach and will become eligible for prizes in the "Security Pays in Many Ways" campaign. F

Continued on page 6.

Stop, thief! That's my identity you're stealing, cont.

Check your financial information regularly and look closely for unusual charges or changes. Closely monitor withdrawals from your bank accounts to ensure that each withdrawal is legitimate.

Consider starting a bill-paying logbook that lists all monthly bills. The logbook should include a section listing all billing company names, their addresses and phone numbers. A monthly section should include the expected bill and last balance. Use this logbook to identify unusual activities such as unknown charges, and to know when bills are due. If you do not receive a monthly statement, you'll know it by the logbook, and you'll know whom to contact to find out why.

If you discover that your statements are being mailed to an address that you have not authorized, inform the billing company immediately. You should now be suspicious that identity theft may be occurring.

Protect your personal bank checks. Do not have your driver's license number or your Social Security number printed on your checks. This may result in more store clerks asking for identification, but if they do, surprise them by thanking them. After all, they are helping you to protect your account.

When you order new checks, you should have them sent to your financial service center to avoid allowing someone to steal them from your mailbox. When storing your extra blank checks, protect them in a safe or secret hiding place.

If you place financial information on your personal computer, consider having all of the sensitive data stored on removable media such as a floppy disk or CD — not on your hard drive. Then, when you decide to sell your computer or send it in for servicing, unauthorized persons cannot gain access to your data.

What should I do if I suspect identity theft?

If you suspect someone else is using your identity, contact your local police department and speak to law enforcement personnel about your suspicions. Then follow their recommendations. If you have enough data, insist that a police report be filed.

Contact your local Post Office if you suspect an identity thief has submitted a change-of-address form or if you suspect someone has used the mail to commit theft or fraud. Contact the Social Security Administration if you suspect that your Social Security number is being fraudulently used (800) 269-0271. Contact the Internal Revenue Service if you suspect the improper use of your identification in conjunction with any tax matter (800) 525-6285.

If you would like to learn more, Day & Zimmermann Protection Technology Hanford encourages you to use the Internet at home or your local library. Just use your favorite Internet search engine and type in "Identity Theft." Here are some Web sites we have found useful. (Please note the list does not constitute PTH endorsement or approval of their content)

- Federal Bureau of Investigation, <http://www.fbi.gov/>
- Federal Deposit Insurance Corporation, <http://www.fdic.gov>
- Federal Trade Commission, <http://www.ftc.gov>
- United States Postal Inspection Service, <http://www.usps.gov/>
- United States Secret Service <http://www.treas.gov/usss/>. ♦