

Tip of the Week

March 7, 2005



Protecting your I.D.

According to a study commissioned by the [Federal Trade Commission](#), last year alone, over 9.9 million Americans learned they'd been victims of identity theft, at a total cost of nearly \$50 billion - an average of almost \$5,000 per victim. Here are some tips that can help you to avoid becoming a victim.

- Avoid giving your SSN to anyone unless absolutely necessary. If someone asks for your SSN, ask:
 - Why do you need it?
 - How will it be used?
 - How do you protect it from being stolen?
 - What will happen if I don't give you my SSN?

If you don't provide your SSN, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to these questions will help you decide whether you want to share your SSN with the business. The decision to share is yours.

- Don't carry your SSN card; leave it in a secure place.
- Do not have your SSN pre-printed on your checks, you can write it on later if absolutely necessary.
- Instead of signing the back of your credit cards, write "Verify I.D." in the signature box instead. This way, merchants "should" request to see a separate piece of signed I.D. before accepting your card.
- The next time you order checks, omit your first name and have only your initials and last name put on them. If someone takes your check book they will not know if you sign your checks with just your initials or your first name, but your bank will know how you sign your checks.
- When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the "For" line. Instead, just put the last four numbers. The credit card company knows the rest of the number.
- Put your work phone number on your checks instead of your home phone. If you have a P.O. Box, use that instead of your home address.
- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or are sure you know who you're dealing with.
- Before you share any personal information on-line, check the organization's website by typing its URL in the address line, rather than cutting and pasting it. Never give information through a link that you jumped to from an email.
- Carry a copy of your passport on your person when you travel abroad, and keep another copy at home in a secure place.
- Make a copy of the front and back sides of all of your credit cards, driver's license, etc. You will have a copy of all of your account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place.
- If you lose your wallet...
 - Cancel your credit cards immediately. The key is having the toll free numbers and your card numbers handy so you know whom to call. Keep those where you can find them easily (obviously, not in your wallet).

- If it is stolen, file a police report immediately in the jurisdiction where it was stolen. This proves to credit providers you were diligent, and is a first step toward an investigation (if there ever is one).
- If you had a company card that was lost or stolen, contact accounting as soon as possible.
- Call the three national credit reporting organizations immediately to place a fraud alert on your name and Social Security number. The alert means any company that checks your credit knows your information was stolen and they have to contact you by phone to authorize new credit.

Credit Reporting Companies

[Equifax](tel:1-800-525-6285): 1-800-525-6285

[Experian](tel:1-888-397-3742): 1-888-397-3742

[Trans Union](tel:1-800-680-7289): 1-800-680-7289