

Protect Your Good Name

Guard against identity theft!



- When shopping online, look in the lower right hand corner of your browser window. If you see a small image of a lock, you are on a secure site. If you don't see one, find another website to buy from. Also, check out website privacy policies. Stay away from those that don't specifically say that they will not share you information with other companies.
- Stick to well-known online retailers or websites that others have used to their satisfaction. Use one specific credit card for your online shopping. That way, if something goes wrong, it will be easier to find on your bill.
- Protect your personal information when filling out forms of any kind. Ask clerks and others if information such as a Social Security number or driver's license is absolutely necessary. Anyone who does require your Social Security number — for instance, your insurance company — should explain their privacy policy and tell you whether you can arrange for the organization not to share that information with anyone else.
- If you get unknown emails, they may be from someone randomly “phishing” for potential targets. Don't open or click anywhere on the email; just use your delete key to get rid of the message and then empty your email trash.

- Sign up for the National Do Not Call Registry to reduce unwanted sales calls. The website is www.donotcall.gov. If you do not use the internet, you can register by phone (1-888-382-1222). Cell phones can also be registered. You remain on the Do Not Call List until you ask to be removed.

- Order your free credit reports each year and review them for suspicious activity. If you spot something suspicious, alert your credit card company or the creditor right away.

If someone is using your identity

Contact the fraud department of **any one** of the three major credit bureaus and tell them. (They will inform the other two.) Ask that a “fraud alert” be placed in your file, along with a statement asking that creditors call you before opening any new accounts or changing your existing accounts.

Equifax Fraud Line: 1-800-525-6285
Experian Fraud Line 1-888-397-3742
TransUnion Fraud Line: 1-800-680-7289

Find more identity theft information and links at www.ct.gov/dcp. Search “identity.”

State of Connecticut
Department of Consumer Protection
165 Capitol Avenue
Hartford, CT 06106

Toll-free: 1-800-842-2649



Identity theft is booming

Americans are facing an attack on their privacy and personal information unlike never before. The identity of an estimated 10 million Americans is stolen each year.

This broad field includes a number of privacy crimes, including theft of a Social Security number, credit or debit card, or even the pilfering of phone calling cards.

Totally shielding your privacy may be close to impossible, but it's helpful to understand how your privacy can be compromised. A few simple measures may improve the odds in your favor.

How it can happen

A great deal of identity theft still comes down to hands-on mischief — and thieves change their tricks constantly. But 80% of victims who call the Federal Trade Commission's Identity Theft Program say they have no idea how it happened.

Obviously, the Internet has opened new avenues for theft by allowing thieves to send and retrieve stolen data to and from most anywhere in the world.

Popular scams involve fake lenders who dangle super low rates if the applicant is quick to provide personal data.



Still others use phone calls or emails in which the criminal poses as a bank or government agency asking the recipient to verify and provide account information.

A lost or stolen wallet containing a Social Security card lets a criminal quickly set up dummy bank and savings accounts, and even apply for a credit card. From there, the con artist may waste little time maxing out the card.

Ways to protect yourself

There is no protection that fully guarantees you'll never fall victim to some form of identity theft. But there are steps you can take to shield your privacy, many of which are rather simple.

- Destroy private records and statements. Tear or shred credit card statements, solicitations and other documents that contain private financial information.

- Empty your mailbox promptly so no one has a chance to steal your mail. Don't leave outgoing mail (such as paid bills that include account numbers) in your mailbox for any passerby to take. Put your outgoing mail in a U.S. Postal Service mailbox.
- Don't carry your Social Security card with you all the time. Take it with you only when you will need it. The same applies to Medicare and Medicaid cards. Leave them in a safe place when you're not using them.
- Don't put your social security number on your checks. Leave your driver's license number off your checks as well.
- Never leave ATM or credit card receipts behind after you withdraw cash or pay for something.

- Pay with cash as often as possible, and pay attention to what store clerks and waitstaff do with your card when they ring up your purchase.

