

## 10 Ways to Stop Identity Theft Cold

Find out how to safeguard your identity in a world of Dumpster divers, mail thieves and shoulder surfers. Plus: What to do if your identity is stolen.

Americans are facing an attack on their personal and financial privacy unlike that seen by any prior generation.

Shielding your private financial information with no risk of a breakdown may be impossible these days. But its critical to understand how your privacy can be compromised and the consequences of such a breach -- and take a few simple steps to, if nothing else, better the odds in your favor.

### Identity theft booming

This rather broad term takes in any number of privacy crimes, including theft of a Social Security number, a credit or debit card, or even the pilfering of phone calling cards.

The numbers associated with identity theft are beginning to add up fast. A recent General Accounting Office report estimates that as many as 750,000 Americans are victims of identity theft every year. And that number may be low, as many people choose not to report the crime or, for that matter, even know theyve been victimized.

Officials say much of identity theft still comes down to hands-on mischief -- things like Dumpster diving, in which criminals sift through trash to find a credit-card statement or solicitation that someone didnt tear up, and 'shoulder surfing', where criminals try to spot calling card and personal identification numbers, and more commonly, mail theft.

Knowing which tricks thieves prefer remains an unquantifiable mystery. Eighty percent of the victims who call us say they have no idea how it happened, says Joanna Crane, program manager of the Federal Trade Commissions Identity Theft Program.

Officials also acknowledge that the Internet has opened new avenues for theft. If nothing else, the Web allows thieves to send stolen data to most any worldwide location.

### How it can happen

One popular scam involves fake mortgage brokers who dangle super low rates if the applicant is quick to provide personal data. Another uses e-mails in which the sender poses as an Internet service provider asking for information: Even though people are told that ISPs will never ask for your Social Security number, one scam was just shut down after 70,000 people responded to their e-mails, notes Crane.

More recently, criminals use email to link consumers to phony Web sites that ask users to "confirm" their account information by entering it into an official-looking online form. (For more on this newest wrinkle in identity theft, see "[Phishing' scams: How to avoid getting hooked.](#)")

Then, there's the infamous skimmer. A skimmer is about the size of a credit card, says Ellen

Moriwaki, a senior product manager at CyberSource, a payment processing and risk management concern. And a criminal buys off a waiter in a restaurant. When you give him your credit card, he rings it up but also runs it through the skimmer, which collects your credit card information. In exchange for \$50 a card, a waiter can gather as many as 100 credit cards a night.

A Social Security card can also reap long-term fraudulent benefits. Virgil Gardaya, a corporate vice president with the credit bureau Equifax, notes that a stolen wallet containing a Social Security card lets a criminal quickly set up dummy bank and savings accounts. The very presence of the account may prompt the bank to give the criminal a credit card. From there, the con artist may waste little time maxing out the card, or take a bit more time and build up the card's buying power. That can mean fraudulent purchases as pricey as cars and boats.

When I moved five years ago, I was alerted that two new accounts had been opened up under my name, adds Gardaya. They actually had statements being delivered to two different addresses.

Simple ways to protect yourself

There's no ironclad protection that guarantees that you'll never fall victim to some form of identity theft. But there are steps you can take to protect yourself, many of which are rather simple:

1. **Destroy private records and statements.** Tear up -- or, if you prefer, shred -- credit card statements, solicitations and other documents that contain private financial information.
2. **Secure your mail.** Empty your mailbox quickly, lock it or get a P.O. box so criminals don't have a chance to snatch credit card pitches. Never mail outgoing bill payments and checks from home. They can be stolen from your mailbox and the payee's name erased with solvents. Mail them from the post office or another secure location.
3. **Safeguard your Social Security number.** Never carry your card with you, or any other card that may have your number, like a health insurance card. And don't put your number on your checks. It's the primary target for identity thieves because it gives them access to your credit report and bank accounts. (For more on protecting your Social Security number, see "[Safeguard your Social Security number](#).")
4. **Don't leave a paper trail.** Never leave ATM, credit card or gas station receipts behind.
5. **Never let your credit card out of your sight.** Worried about credit card skimming? Always keep an eye on your card or, when that's not possible, pay with cash.
6. **Know who you're dealing with.** Whenever anyone contacts you asking for private identity or financial information, make no response other than to find out who they are, what company they represent and the reason for the call. If you think the request is legitimate, contact the company yourself and confirm what you were told before revealing any of your personal data.
7. **Take your name off marketers' hit lists.** In addition to the national [Do-Not-Call registry](#) (1-888-382-1222), you can also cut down on junk mail and opt out of credit card solicitations. For details, see Liz Weston's article, "[Free at last from telemarketing invasions](#)."

**8. Be more defensive with personal information.** Ask salespeople and others if information such as a Social Security or drivers license number is absolutely necessary. Ask anyone who does require your Social Security number -- for instance, your insurance company -- what their privacy policy is and whether you can arrange for the organization not to share your information with anyone else.

**9. Monitor your credit report.** Obtain and thoroughly review your credit report (now available for free at [Annualcreditreport.com](http://Annualcreditreport.com) or by calling 877-322-8228) at least once a year to look for suspicious activity. If you spot something, alert your card company or the creditor immediately. You may also want to subscribe to a credit protection service, like Experian's [CreditCheck](#), which alerts you any time a change takes place with your credit report.

**10. Review your credit card statements carefully.** Make sure you recognize the merchants, locations and purchases listed before paying the bill. If you don't need or use department-store or bank-issued credit cards, consider closing the accounts. For more on when and how to close credit card accounts, see "[Cancel a credit card -- the right way.](#)"

If something goes wrong

Again, protecting yourself from identity theft is no sure thing. But there is plenty you can do if you uncover some wrongdoing:

First, contact the fraud departments of each of the three major credit bureaus. Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, along with a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts.

**Equifax**

To report fraud: 1-800-525-6285  
and write: P.O. Box 740241, Atlanta, GA 30374-0241

**Experian**

To report fraud: 1-888-EXPERIAN (397-3742)  
and write: P.O. Box 9532, Allen, TX 75013

**TransUnion**

To report fraud: 1-800-680-7289  
and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634

Contact the creditors for any accounts that have been tampered with or opened fraudulently. Speak with someone in the security or fraud department of each creditor, and follow up with a letter.

File a report with your local police or the police in the community where the identity theft took place. Get a copy of the police report in case the bank, credit-card company or others need proof of the crime.

Keep records of everything involved in your efforts to clear up fraud, including copies of written correspondence and records of telephone calls.