

Protecting Yourself from Identity Theft

There are several ways someone can get hold of your personal information: dumpster diving at a business that has your information, digging through your home garbage, stealing mail, skimming your credit card at a store, and outright mugging you and taking your wallet or purse.

Once someone has your information, it can take almost no time to open accounts in your name, and charges on your credit and debit cards can appear almost immediately. To make matters worse, the thief usually knows what they're going to buy before they get your cards.

An identity thief can also steal those pesky pre-approved offers you get and open accounts that way. Or they can steal a credit card statement that contains all your information, and file a change of address — which might take you a while to realize you are a victim.

THE IRS WANTS WHAT?

Another way thieves can steal your identity is by sending you an official-looking e-mail that says it is from the IRS, your bank or some other government agency. They ask you to verify personal information for a variety of reasons, but these e-mails are almost always a scam.

The IRS does not contact people by e-mail or phone, and neither do other government agencies and most banks. If an agency does need to get hold of you, they will do so by mail and await your response.

PROTECT YOURSELF

There are several relatively easy ways to help protect against identity theft.

Identify theft is a frightening and costly issue. Do you shred important documents like bank statements, insurance documents and the like before you throw them out? If not, you could be setting yourself up for identity theft. Identity theft is a crime of opportunity. And it can be as easy as picking through your garbage. Don't let anything leave your house in one piece; buy a shredder.

There may be other ways of doing business without having to turn over certain information.

1. Buy a shredder. Cross cut shredders are preferable and can be purchased anywhere, from OfficeMax to Target, for around twenty dollars
2. Minimize what you carry on you. DO NOT carry your Social Security card, Medicare card or more credit cards than absolutely necessary. If you need to show a Medicare card for medical care, make a copy and black out all but the last four numbers. If going to your regular doctor or pharmacy, they should already have you in the system and can look you up that way. If using a new service, it's okay to take your original card on the first visit — then make a copy.
3. Read bank and credit card statements and credit reports carefully. If you notice something suspicious call the company and have your account frozen immediately.
4. Be wary of "official" looking e-mails. Government agencies and banks do not contact people this way.
5. When you must give personal information, ask why it is needed, how the company will protect it, and what will happen if you refuse.

If you do find yourself a victim of identity theft:

1. Place a fraud alert on your credit reports and review them carefully.
2. Close accounts you know or believe have been tampered with or opened by someone other than you.
3. File a police report and notify the Federal Trade Commission. You can find information about reporting identity theft at ftc.gov.

Many credit card companies will not hold you liable for fraudulent expenses if you can prove you were a victim. Unfortunately, many banks will not reimburse you for money lost, but check with your individual banks for its policies.

Awareness is an effective weapon against many forms identity theft. Be aware of how information is stolen and what you can do to protect yours, monitor your personal information to uncover any problems quickly, and know what to do when you suspect your identity has been stolen.

To learn more about identity theft, visit www.ftc.gov