How Can I Protect Myself from Identity Theft?

Identity theft remains one of the most personal crimes. Someone finds pieces of your financial information and essentially uses them to become you – charging up a boatload of goods and services in the process.

Though identity theft fell by nearly 30 percent in 2010, according to Javelin Strategy and Research, you should always think about it, and safeguard your personal financial information.

Here are ten simple ways to protect yourself against identity theft:

1. **Protect your credit cards.** Make sure you know where all of your credit cards are. Keep them locked up when you're not using them. If you have cards that are inactive accounts, destroy them. Check the accounts of your active cards weekly to see if there are charges you don't recognize.
2. **Be careful where you use your debit card.** Debit card fraud rose in 2010. Check to see if the bank issuing your debit card provides zero-liability protection if a card is ever lost, stolen or used without authorization. Zero-liability protection makes sure you're not responsible for unauthorized or false charges on your account. Report lost or stolen cards or suspected fraud immediately. If you don't, you could wind up being responsible for the charges against your account.
3. **Protect your Social Security number.** NEVER carry your Social Security card in your wallet. Your Social Security number is key to many of your financial accounts. If someone gets your Social Security number, you may be in big trouble. You have to protect it even more so than your credit cards—make sure your Social Security card is kept in a safe place. Ask what your employer is doing with your Social Security number as well. Employers only need your Social Security number for reporting to the IRS; it does not need to be on internal work documents. And when you go to a new doctor or dentist, do not provide your Social Security number. The medical office does not need it.
4. **Use the postal service as little as possible.** One reason the post office is losing business is that mail is one of the most vulnerable sources for identify theft. If possible, have bills sent electronically. If a bill goes missing, immediately contact the company to find out what happened to it. A thief can easily take one of your bills and change your address to make sure you don't see your next bill with fraudulent charges. Also, avoid mailing checks to pay bills or deposit funds into your checking account. Instead, use online bill payment whenever you can. Doing personal business online can be totally secure, if you manage it correctly.
5. **Be careful what you put on your résumé.** DO NOT include your Social Security number, birth date, driver's license number, reason you left a past employer or even marital status on a résumé. Consider leaving off graduation dates and other personal information. You'd be surprised at how much a thief can do when armed with the smallest pieces of personal information.
6. **Limit how much personal information you share on social networking sites.** Don't put too much information—your street address or full date of birth, for

example—in your online profile. Don't put the year of your birth on Facebook or any other site. Be aware of privacy controls on social networking sites like Facebook, and restrict access to people you don't know. Similarly, don't allow someone you don't know to have access to your page.

7. **Monitor your credit history.** Get a free copy of your credit report at www.annualcreditreport.com. Look for strange numbers, new credit cards you never opened, late payments, judgments against you that aren't yours or other information that seems wrong. Keeping an eye on your credit report is one of the fastest ways to discover that your identity has been stolen.
8. **Be careful whenever you use your ATM card or credit card.** Watch who's watching you when you withdraw money out of an ATM machine. Don't let lurkers pick up your PIN. Also, don't keep your PIN written on your card or on a slip of paper in your wallet.
9. **Properly dispose of sensitive documents and equipment.** Shred old documents and applications for credit cards you get in the mail. Your computer can also be a target because it contains a lot of valuable information that can be hacked. If you get a new computer, don't just throw out the old one in the trash. Be sure you wipe the hard drive clean or find a reputable place to dispose of your electronics. The same goes for your cell phone.
10. **Learn about identity protection services.** You may want to consider signing up for a credit monitoring service in order to protect yourself. Look for a trusted, established company with trained fraud specialists. You can also set up fraud alerts on your credit report. These alerts ask your credit grantors to contact you before giving you a new account. Another option is to set up a credit freeze with the three national credit reporting bureaus. Freezing means that no one new can open an account or look at your file. It does not close your existing lines of credit. Consider freezing your account if you think your personal information has been compromised.