Protecting Your Privacy

As a consumer, you give out personal information in many situations. When you open a bank account, apply for a credit card, or fill out a form on a Web site, you provide information about yourself and your finances. Companies can even gather information about you based on the Web sites you visit. In the practice known as online profiling, these companies use cookies, small files stored on your computer, to record information about you. They use that information to tailor online advertising to your interests.

Many consumers are concerned about giving out personal information, and about how that information is used. They don't want other companies to know about their purchasing habits. They don't want to be bombarded with catalogs and e-mails about gardening just because they bought gardening tools from a Web site. In other words, they want to protect their privacy.

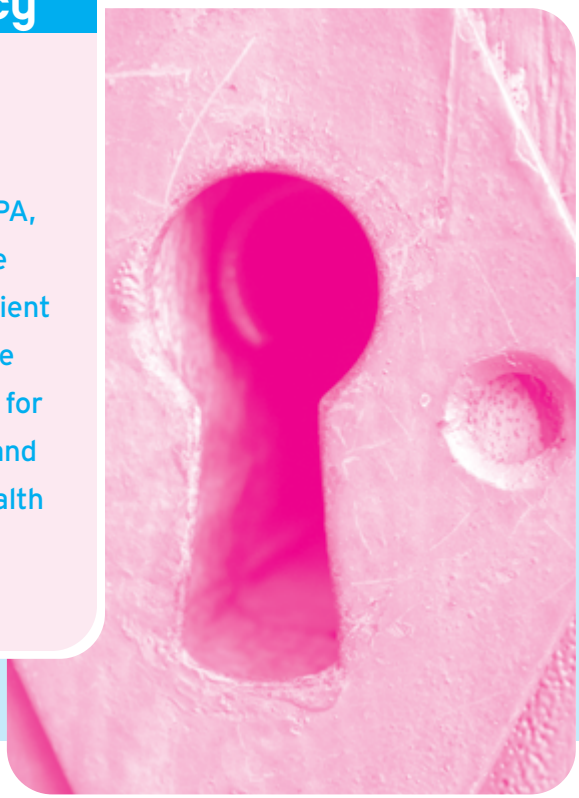
Fortunately, the government is on your side. It has introduced laws requiring all companies involved in financial activities to send their customers privacy notices. The notices explain company policy regarding customer privacy, and give you the right to opt out of having your information shared with others. In general, if you don't opt out, the company will assume that it can share your information.

The Opt-in Option

Some companies have an opt-in policy. They agree not to send you e-mails or promotional materials unless you opt in, or specifically give your consent. If you choose to opt in, and then change your mind later, you can always opt out again.

Health Care Privacy

Concern about consumer privacy extends to health care too. The Health Insurance Portability and Accountability Act, known as HIPPA, includes safeguards to protect the security and confidentiality of patient information. It requires health care companies to use secure systems for transmitting patient information and forbids the disclosure of some health information without the patient's authorization.



PREVENTING IDENTITY THEFT

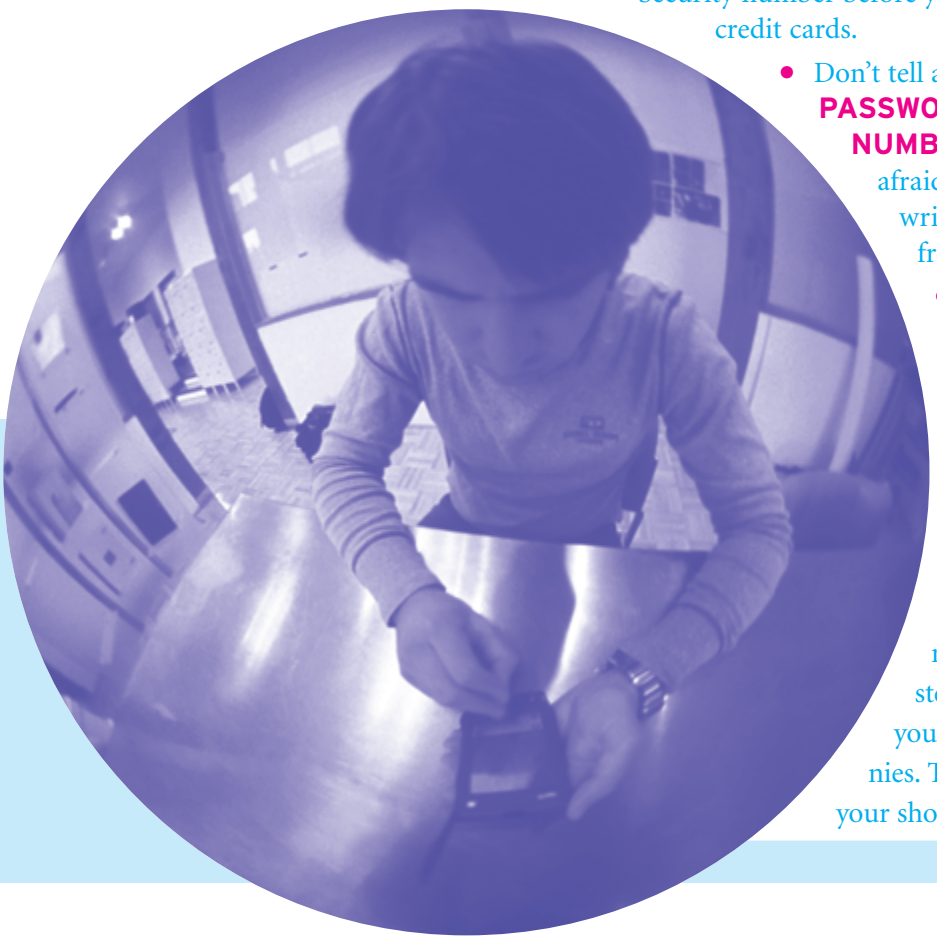
One reason consumers are concerned about their privacy is that they fear identity theft—the illegal use of their personal information by a complete stranger. Identity theft begins when someone gains access to information such as your name, social security number, date of birth, credit card number, PIN number, and so on.

How does this happen? Identity thieves might steal your wallet or purse containing credit cards, steal your mail (lots of personal information there), or retrieve discarded papers from your garbage. They might watch over your shoulder when you use an ATM, steal personal information from the Internet, or use a number of other methods to gain information. Once they have the information, they might use your credit card to run up charges, open new credit card accounts in your name, and generally cause financial havoc for you. Victims of identity theft sometimes spend years setting the record straight.

To avoid identify theft take these precautions:

- Don't give out your **SOCIAL SECURITY NUMBER** unless you must, and then only to people or organizations you know you can trust.
- When you need to give personal and financial information over the Internet, check that you're at a **SECURE SITE**.
- **TEAR UP OR SHRED** bank statements, credit card statements, and any other documents that might contain account numbers and/or your Social Security number before you throw them away. Cut up expired credit cards.
- Don't tell anyone your computer or online **PASSWORD**. Don't tell anyone the **PIN NUMBER** for your debit card. If you're afraid of forgetting the number and must write it down, keep it in a separate place from the card.
- Make sure no one is watching you when you use an **ATM**. Likewise, be aware of your surroundings when you use your **CELL PHONE**. Don't give out personal information by phone when somebody might overhear you.

If you ever suspect that your identity has been stolen you will need to act immediately. Your first steps should be to contact the police, your bank, and your credit card companies. They will advise you on the actions your should take next.



QuickTip

Keep a List

Be prepared for identity theft. Keep a list of account numbers from credit card companies, banks, and other financial service providers in a safe place at home. That way, if you become a victim of identity theft you can quickly call the companies and providers to stop action on your account.

Welcome to the
REAL WORLD

An Easy Target

IT ONLY TOOK A SECOND. Tina put her purse down by her feet as she tried on hats in the store. When she went to pick it up, it had gone. The store manager was very helpful. He called the police and suggested that while Tina was waiting for them to arrive she list the contents of her purse. Here's what Tina listed: $60 in cash; checkbook; debit card; bank credit card; four store credit cards; gasoline credit card; Social Security card; driver's license. When the police arrived and questioned her, she admitted that she also kept the PIN number for her debit card written on a small piece of paper in her purse.

YOUR IDEAS

1. What made Tina an easy target for an identity thief?

2. What changes should she make to the items she keeps in her purse?

3. Based on what you learned in this exercise, what changes should you make to the way you store your personal documents?