Fraud and identity theft incidents claimed fewer victims in 2010 than in previous years.

But don't get too comfortable. Average out-of-pocket consumer **costs** for these incidents were **higher** than ever.

Are you doing everything you can to protect yourself?

Read on for valuable **tips to safeguard** against fraud and identity theft.

Trends & Tactics

IDENTITY THEFT

Identity theft occurs when your personal information is stolen and used to acquire bank or credit card accounts, secure loans, establish utility services or even get a home mortgage. Such information may include your address, phone number, Social Security number, bank or loan account numbers, user names, passwords, etc.

PHISHING/VISHING

Fraudsters may pose as a trusted financial institution, ATM/debit network, online retailer or other service provider to trick individuals into disclosing private information. Typically, you receive an unsolicited email or phone call asking you to verify personal or financial information. HTML webpage attachments are the latest trend, and may be able to bypass common security mechanisms.

PHARMING

Pharming uses computer software, such as crimeware, malware or spyware, to collect personal information from your computer and deliver it to fraudsters. When you attempt to log on to a legitimate website, you are unknowingly redirected by the fraudulent software to an authentic-looking but bogus site. Criminals then capture and use the personal information you enter. Since the redirect happens behind the scenes, pharming is extremely difficult to detect.

OTHER CRIMINAL TECHNIQUES

- Stealing account statements, pre-approved credit offers, checks and tax information from your mailbox
- Obtaining your credit report by posing as someone who may have a right to such information
- Filling out change of address forms to reroute mail
- Finding personal information in your home or trash
- ATM tampering and fraud, such as shoulder surfing, card skimming and card slot or keypad alterations

How to Safeguard Yourself

TREAT UNSOLICITED OFFERS WITH SUSPICION

If you receive a request or offer via email, pop-up message or phone call that requires you to provide or confirm personal information, do not respond. Instead, call the business using a different phone number (on the back of your card or on your monthly statement) to confirm the legitimacy of the request or offer.

SHOP CAREFULLY ONLINE

If you initiate an online transaction and must provide personal data, type the URL into your browser instead of using a link. Look for indicators that the site is secure, like "https" in the web address or the closed padlock icon in your browser. It also is wise to conduct financial transactions on wired Internet connections. Wireless connections can be more vulnerable to attack.

USE UPDATED ANTI-VIRUS SOFTWARE, ANTI-SPYWARE AND A FIREWALL

Some phishing and pharming attacks contain software that can harm your computer or track your activities on the Internet without your knowledge.

REVIEW ACCOUNT STATEMENTS REGULARLY

Verify all transactions by matching receipts to your account statements. Frequently reviewing accounts online helps identify unauthorized activity between monthly statements. Many financial institutions offer free email alerts for routine account activity and unusual transactions.

REVIEW YOUR CREDIT REPORT EVERY YEAR

You are entitled to one free credit report each year. You also may obtain a free report at any time if you are a victim of identity theft. To request your free report, log on to **www.annualcreditreport.com** or call **877-322-8228**.

PROTECT YOUR PURSE OR WALLET

One of the leading causes of identify theft is lost or stolen belongings containing personal information. Minimize the number of items you carry that contain personal information, such as your Social Security card.

CLOSE ACCOUNTS

If you become a victim, close all affected accounts immediately to minimize the damage. Change passwords on all other accounts.

OPT OUT

Limit the disclosure of your personal information. Contact your financial institutions, mortgage brokers and the three major credit reporting agencies to opt out of programs that share your information. You also can block inquiries that result in pre-approved lines of credit.

ADDITIONAL STEPS TO PREVENT FRAUD

- Shred all personal and financial documents before disposing of them
- Destroy unused debit, ATM and credit cards
- Remove mail promptly from your mailbox
- Memorize PINs, passwords and Social Security numbers – do not carry them with you
- Use longer, more complex PINs and change them often
- Use debit and credit cards with your photo when possible
- Never use your PIN as a password
- Never disclose your PIN or account password to anyone for any reason
- Notify creditors and financial institutions of address changes in advance

Signs You May be a Victim

CREDIT SIGNS

Receiving unsolicited credit cards, denial of credit or less favorable credit terms may be an indication of identity theft. Check your credit report to determine if you are the victim of a crime and assess the extent of the fraudulent activity.

MISSING BILLS

Be aware of when your bills typically arrive. A missing bill or statement may be a sign that a thief has changed the billing address or rerouted mail to another address.

UNEXPECTED PHONE CALLS

If you receive phone calls from collection agencies for debt you did not incur, do not give the caller any personal information. Investigate the charges immediately, close the account(s) and report the incident to authorities.

Report Violations

If you think you may be the victim of any form of financial fraud or identity theft, notify the proper authorities immediately.

REPORT ALL PHISHING ATTACKS TO:

INTERNET CRIME COMPLAINT CENTER:
www.ic3.gov

FEDERAL TRADE COMMISSION:
Forward all potentially fraudulent email to spam@uce.gov.

Report violations of your personal information and debit or credit card theft to your account providers immediately. You should also notify the three major credit bureaus:

Experian 888-397-3742
Equifax 800-525-6285
TransUnion 800-680-7289

For more information, visit DebitSavvy.org