IDENTITY THEFT : *WHAT TO KNOW AND WHAT TO DO*

Developed by Dr. Ashok Sapre

In the electronic age, identity theft has become a major problem. Last year over 16 million households fell victim to identity theft. It is a serious crime. It can disrupt your finances, credit history, reputation, and even create serious problems in getting proper medical services including medical insurance. It takes time, money, and patience to resolve the situation. Identity theft happens when someone steals your personal information and uses it without your permission to assume your identity.

There are several symptoms to suspect that your identity might be stolen: 1. Mistakes on your bank, credit card, or other account statements. 2. Mistakes on your medical benefits from your health plan. 3. Your regular bills and account statements don't arrive on time. 4. Bills or collection notices for services that you never received. 5. Calls from debt collectors about debts that don't belong to you. 6. A notice from the IRS that someone used your Social Security number. 7. Businesses turn down your checks. 8. You are turned down unexpectedly for a loan.

Any one of these situations is good reason for you to suspect that you might be a victim of identity theft.

If Your Identity is stolen....: 1. Flag your credit reports. Call one of the nationwide credit reporting companies, and ask for a fraud alert on your credit report. The company you call must contact the other two so they can put fraud alerts on your files. An initial fraud alert is good for 90 days. Equifax: 1-800-525-6285; Experian: 1-888-397-3742; TransUnion: 1-80carefully to see if the 0-680-7289. 2. Order your credit reports. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact the credit reporting company. 3. Create an Identity Theft report. An identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft report file a complaint with the FTC at ftc.gov/complaint or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit. Take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

The two documents comprise an Identity Theft report.

Most Common Ways How Your Personal Information Is Stolen: 1. Going through your trash cans and dumpsters, stealing bills and documents that have sensitive information. 2. Stealing personal information on the job by employees who work for businesses, medical offices, or government agencies that handle personal information. 3. Stealing your wallet, purse, backpack, or mail, and remove your credit cards, driver's license, passport, health insurance card, and other items that show personal information. 4. Pretending to offer a job, a loan, or an apartment, and ask you to send personal information to "qualify". 5. Hacking business or government agencies electronic data systems that store your personal information.

How to Protect Your Information: 1. Read your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or order one report every four months. To order, go to www.annualcreditreport.com or call 1-877-322-8228. 2. Read your bank, credit card and account statements, and the explanation of medical benefits from your health plan. If a statement has mistakes or doesn't come on time, contact the business. 3. Shred all documents that show personal, financial, and medical information before you throw them away. 4. Don't respond to email, text, and phone messages that ask for personal information. Delete the messages. 5. Create passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account. 6. If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address; "s" is for secure. 7. If you use a public wireless network, don't send information to any website that isn't fully encrypted. 8. Use anti-virus and anti-spyware software, and a firewall, on your computer. 9. Set your computer's operating system, web browser, and security system to update automatically.

Medical ID Theft: Medical ID thieves may use your identity to get treatment—even surgery—or to bilk insurers by making fake claims. Medical ID theft can have serious consequences for your health care services. If a scammer gets treatment in your name, that person's health problems could become part of your medical records. It could affect your ability to get medical care and insurance benefits, and even affect decisions made by doctors treating you later on. If you are alert you can catch medical ID theft early on. First, read every "Explanation of Benefits" statement you get from your health insurer. Follow up on any item you don't recognize. At least once a year, ask health insurers you have been involved with a list of the benefits they have paid in your name.