

IDENTITY THEFT
BY
JOHN STRESSMAN, CHIEF OF POLICE

The following information was obtained from training materials provided by ID Safety®, The International Association of Chiefs of Police® and Bank of America®.

Identity crime is the fastest growing crime in the United States with over nine million victims annually. This crime will impact one out of every four people. Visit www.idsafety.org today to get your free identity crime prevention kit.

Identity crime is a crime where a suspect gains access to your personal information and/or account numbers, then assumes your identity and goes on a spending spree, commits a crime in your name, or does any of a number of other things while posing as you.

It is an unusual crime in that you often do not realize you are a victim until long after the perpetrator has started to use your identity to do his/her crimes. Often victims discover the crime after they receive a bill, collection notice, or a telephone call in reference to an attempt to make a large purchase, such as a car. Then they realize their credit has been destroyed.

Once victimized, people end up spending money out of pocket to clear up their records, but they also must devote their time—hundreds of hours in some cases—doing so. In the meantime, the victims are unjustly harassed by debt collectors, denied credit or employment opportunities, and in some cases, even lose their cars or homes.

You do not have to be a victim of identity crime for personal information to fall into the wrong hands. In the course of a busy day, how often might you share information about yourself in person, on the phone, or over the Internet? Although it is impossible to guarantee that identity crime will not happen to you, there are ways to reduce your chances of becoming a victim. Most victims do not discover the crime until it is too late. It can take a long time to reverse the damage these criminals can do to your credit rating.

Any of these indicators could mean that you have become a victim of identity crime:

- Mysterious bills for accounts you are not aware of
- Phone calls from creditors about delinquent payments you do not recognize
- Mail from unknown lenders asking for additional information

Preventing Identity Theft:

Carry only necessary identification and credit cards with you. Do not carry your Social Security card; treat your credit cards and check (debit) cards like cash; and do not carry any personal identification numbers (PIN's)—memorize them. Make copies of all of the financial information that you carry with you daily and store the copies in a safe place.

And, retrieve incoming mail from your mailbox quickly, and do not leave outgoing mail, like bill payments with checks, in an unsecured mailbox or other location.

If you cannot verify the identity of the person or business asking for your personal information, be very cautious about the transaction. If you do not understand why a certain piece of information is needed, think twice about the transaction; and be cautious of telephone and door-to-door solicitations.

Never provide personal or financial information unless you initiated the contact and you have confirmed the business's or person's identity. Ignore offers that seem "too good to be true." They usually are.

Provide sensitive personal information like Social Security Numbers or account numbers only to people or businesses you trust, and who have legitimate reasons to ask for it. Be very suspicious of e-mails requesting your personal information for "account verification" or other reasons. Almost no legitimate companies do this. Never click on a link within such an e-mail. If you want to go to a site, type the Web addresses into your Web browser yourself.

Reduce the amount of mail you receive that display personal information by not receiving account statements in the mail. Many financial institutions offer electronic delivery of statements, and many companies will send your bill electronically, as well. Check with your financial institution for details. Paying bills online also eliminates the security risk of mailing paper checks, as does not having canceled checks mailed to you. Many financial institutions allow you to view canceled checks online. Signing up for direct deposit to have your paychecks, dividends, tax refunds, and other deposits sent directly to your account without the need for a paper check is a good idea. Opt out of pre-approved credit card offers by calling 1-888-567-8688. This will communicate your preference to all three of the major credit bureaus.

Shred all financial documents, including credit card and other financial solicitations, before recycling or throwing them away.

Install anti-spyware, anti-virus, and a personal firewall on your computer and update them regularly, especially virus and spyware definitions. Either schedule regular anti-virus and anti-spyware scans, or make it a habit to do it manually. Update your operating system and browser regularly. Their makers identify potential security problems and issue "patches" to fix them.

Choose pass codes and personal identification numbers (PIN's) that are difficult for others to guess. If possible, use a combination of lowercase and capital letters, numbers, and symbols. Use a different pass code for each of your online accounts and always log off from online sessions with your banking or bill payment providers, or other sites where you interact with personal information—a preferred tactic is to completely close the window after exiting the site.

Be vigilant and suspicious in your online activities and monitor your online accounts regularly. Remember that forging e-mail and creating fraudulent websites is easy to do, and if you are at all suspicious, leave the site immediately.

If you believe you are the victim of identity theft, or if you have received suspicious communications which you believe are intended to compromise your personal and financial information, contact the police department in your jurisdiction to report the incident. An officer or deputy can give you information on what courses of action to take to stop potential or further loss.