Title:
Protect Yourself from Identity Theft

Word Count:
1441

Summary:
Some law-enforcement authorities call identity theft the fastest growing crime across the country right now. In fact, identity theft is the most called-about subject on the Privacy Rights Clearinghouse's telephone hotline. Most victims don't even know how the perpetrators got their personal information.

Keywords:
personal security, security, identity theft, fraud, theft, crime, cybercrime, cyber crime, identitytheft, id, identity, steal, stolen, secure, personal information, computer, internet, security, safety, safe, secure, tips, tricks, how to, credit, pro

Article Body:

Some law-enforcement authorities call identity theft the fastest growing crime across the country right now. In fact, identity theft is the most called-about subject on the Privacy Rights Clearinghouse's telephone hotline. Most victims don't even know how the perpetrators got their personal information.

Such fraud may account for as much as 25% of all credit card-fraud losses each year. Not surprisingly 49% of the victims, who have had their identities stolen, stated that they do not feel they know how to adequately protect themselves from this crime.

What Steps Can you Take to Avoid Identity Theft?

1. Credit Report

Order your credit report each year from each of the three major credit reporting agencies. Check each credit report carefully for accuracy and for indications of fraud, such as credit accounts that you did not open; applications for credit that you did not authorize; credit inquiries that you did not initiate; charges that you did not incur; and defaults and delinquencies that you did not cause. Check the identifying information in your credit report to be sure it is

accurate pay particular attention to your identifying information like your name, address, and Social Security number. Make sure that you recognize every line of information established in your file.

2. Social Security Report

Additionally order your social security earnings and benefit statement once a year so that you can check to make sure your earnings are correctly recorded. If the numbers are inflated it maybe because someone is using your Social Security number for employment. (Note - The Social Security Administration now automatically mails these statements annually to all eligible workers age 25 and older).

3. Checks

Call the payees of any outstanding checks that you are not certain you wrote. The payee is the person or business to whom you wrote the check. Explain to each payee that you are the victim of identity theft and that you have to close your checking account for that reason. Ask each payee to waive (forgive) any late payment or returned check fee. Then send each payee a replacement check drawn on your new account and stop payment on the check that it replaces. It's a good idea to enclose a note with each check explaining why you are sending a replacement check and reminding the payee that the payee has agreed to waive the late payment or returned check fee.

4. Mail

If you are traveling be sure to stop your mail delivery at the post office, rather than having it accumulate unattended in your mailbox. If you do not receive your credit card statement on time or if you do not receive a new or renewed credit card when you expect it, your mail may have been stolen. If you notice your mail is dwindling, check with the post office to see if they have any change of address posted. If a change of address request has not been filed at the post office check if one has been filed with the creditor. Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. Install a lock on your mailbox if you live in an area where mail theft has occurred. This will reduce the risk of mail theft.

5. Good Record Keeping

Be sure to keep a list of all your credit card account numbers, expiration dates, and telephone numbers of the customer service and fraud departments in a

secure place, not in your wallet or purse, so that you can quickly contact your creditors in case your cards are lost or stolen. Make a list of, or photocopy, all of your credit and debit cards. For each card, include the account number, expiration date, credit limit and the telephone numbers of customer service and fraud departments. Additionally be sure to store a list of bank accounts in secure location, along with access numbers.

6. Lost or Stolen

A thief may steal, or the consumer may lose, the consumer's purse or wallet. The thief then may use the consumer's stolen personal identification information to obtain credit in the consumer's name.

7. Collection

If you receive calls from collection agencies or creditors for an account you don't have or that is up to date. Someone may have opened a new account in your name, or added charges to an account without your knowledge or permission. Financial account statements show withdrawals or transfers you didn't make. A creditor calls to say you've been approved or denied credit that you haven't applied for. Or, you get credit card statements for accounts you don't have. You apply for credit and are turned down, for reasons that do not match your understanding of your financial position.

8. Notebooks

Laptops and notebooks are treasure troves of useful information. Be sure to password protect any sensitive information. When creating passwords and PINs (personal identification numbers) do not use any part of your Social Security number, birth date, middle name, spouse's name, child's name, pet's name, mother's maiden name, address, telephone number, consecutive numbers, or anything that a thief could easily deduce or discover. For tips on strong passwords refer to: http://www.password-software.com . Avoid using an automatic log-in feature that saves your user name and password; and always log off when you are finished.

9. ATM/ Credit Cards

If your ATM card has been lost, stolen or otherwise compromised, cancel the card as soon as you can. Get a new card with a new PIN. If you suspect unauthorized use, contact the provider's customer service and fraud departments immediately. Never give out your credit card, bank account or Social Security number over the telephone unless you placed the call and you have a trusted business

relationship with the business or organization. Place passwords on credit cards, bank and phone accounts. Avoid using easily available information like mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. Cancel your unused credit cards so that the accounts will not appear as being "open" or "active" on your credit report. Shield your ATM or telephone key pad when using an ATM or making a phone call with your phone calling card. Some shoulder surfers' use binoculars or video cameras to record your numbers. If you use ABMs or point-of-sale terminals, always shield the entry of your PIN, and never give your access code (PIN) to anyone. Choose a PIN that can't be figured out easily, as you could be liable if you use a PIN combination selected from your name, telephone number, date of birth, address or Social Insurance Number (SIN). Remember that no one from a financial institution or the police will ask you for your PIN. Always take credit card, debit card and ATM receipts with you. Never throw them in a public trash container. ear them up or shred them at home when you no longer need them.

10. Trash

One person's trash is another person's treasure. Shred documents before throwing them away. Be sure to shred credit card statements, bank statements, pre-approved applications, any important papers with identifying numbers. Memorize ALL passwords and PIN numbers. Keep them private. Some thieves create identities by retrieving personal information in your garbage or recycling bin by "dumpster diving".

11. Public Information

Some thieves use public information, Searching public sources, such as newspapers (obituaries), phone books, and records open to the public (professional certifications). Consider not listing your residence telephone number in the telephone book, or consider listing your name and residence telephone number without an address. If you decide to list your name and telephone number, consider not listing your professional qualification or affiliation (for example, "Dr.," "Atty.," or "Ph.D .").

12. Online Banking

After completing a financial transaction or online banking, make sure you sign out of the Web site and clear your Internet file/caches (Internet files are retained in your computer automatically and thus should be cleared so that hackers cannot obtain the information). Most financial institutions provide instructions on how to clear the caches under their "security" section. Look for

"https" in the URL header and a padlock icon on your Internet toolbar at the bottom of the screen; both indicate that a secure connection is in effect. With Microsoft Internet Explorer, click Tools then Internet Options. On the General tab, click Delete Files, Delete Cookies and Clear History buttons.

13. Posing

Do not release any information to anyone calling. Thieves often pose as a creditor, landlord or employer to get a copy of your credit report or access to your personal information from other confidential sources.