Title:
How To Protect Yourself From Identity Theft

Word Count:
901

Summary:
Identity Theft is a real and growing problem. So what is identity theft exactly?
Basically, identity theft is when someone uses your social security number, your
bank credit card number, your driver's license number or any other form of
identity without your knowledge or permission.

Keywords:
id theft,idenity theft,credit repair,card credit,bad credit loan,loan,repair bad
credit,banks,personal finances,finance,auto loan,payday loan,bad credit personal
loan

Article Body:
Identity Theft is a real and growing problem. So what is identity theft exactly?
Basically, identity theft is when someone uses your social security number, your
bank credit card number, your driver's license number or any other form of
identity without your knowledge or permission.

Many people have fallen victim to identity theft through many different means.
Some of these ways are easily preventable due to their common sense obvious
nature. Other ways identities are stolen are more dubious and discreet.

So, the question becomes, how can you protect yourself from someone stealing
your identity?

To protect yourself from identity theft, the first thing you should do when
considering how to divulge information about your identity to someone you do not
know or may not trust is to use your common sense. Never make one-sided
assumptions or take things for granted where your identity is concerned.

Credit card company statements and bank statements you receive in the mail
contain your account information including your account number. Any of these
items need to be shredded with an inexpensive shredder you can buy at any office
supply store. Do not throw credit card statements, old credit cards or bank
statements, etc. in the trash as that presents an easy way for someone going
through the trash to steal your account information and use it as if they were

you.

Another thing you can do to protect yourself against credit card fraud and unauthorized credit card usage is to sign the back of your card as "Check ID". If a store clerk asks to see your card, he or she will check the signature on the back and compare it with some other form of ID you have. This safeguard will not work where a purchase can be automatically completed (like at a gas pump).

When you are buying items at a store or withdrawing money from a bank or ATM machine using your ATM debit card always protect the visibility of your PIN number as you punch it in.

Do not carry your social security card with your number on it in your wallet. Keep your social security card or anything with your social security number on it in a safe place where no one has access to it but you. If you must dispose of anything that has your social security number on it, do not forget to shred it.

When online, do not open files sent to you by strangers or even files that are from someone you know but were not expecting to receive any from them. Do not click on hyperlinks or download programs from people you do not know either. Opening a computer file from an unknown source could expose your system to a computer virus, a Trojan or spyware. These types of programs could be ones that could log your keystroke information containing your credit card numbers, passwords or other sensitive information as you type it in.

If you use Ebay or Paypal, read the company website policies concerning how they handle communication to you about your account information. Never trust an email you may receive out of nowhere from Ebay or Paypal asking you to "update your account information" as this is more than likely a ploy to steal that information and use it illegally.

Use a firewall program and a router while you are online if you have high speed internet that leaves your computer connected to the internet 24/7. The router and the firewall program both make it much more difficult for a hacker to see your computer's actual IP address which means that you have a better chance of safely sending and receiving sensitive information over the internet. Windows XP operating system SP2 has a built in firewall which you should make sure is enabled in your settings.

When you are shopping online, always use a secure browser and shop from a web site that offers secure transactions when shopping online. Most browsers in use today have this protection feature including the popular Internet Explorer and Mozilla Firefox browsers. Secure website shopping carts you visit will show up

as "https://thestoresdomain.com" in the web browser address bar.

Practice keeping your computer clean from spyware or Trojan programs that log keystroke information by using virus protection software and spyware monitoring and removal software. These programs should be updated regularly, and updates for you're operating system and other software programs should be installed regularly to protect against the compromise of your computer files and password information. Ideally, virus protection software should be set to update itself frequently. The Windows XP operating system will update itself automatically if you enable this feature, which you should.

The consequences of identity theft once thieves have your information can be quite severe and range from going on a spending spree to taking out auto loans in your name. For these reasons and others, it is a good idea to monitor your credit report periodically. A credit report can be obtained from Trans Union Corp. New laws have made it easy for you to get at least one free credit report that you can use to see if accounts have been opened in your name.

You may copy this article and place it on your own website, as long as you do not change it and include this resource box including the live link to the Credit Repair Advice site.