“Identity Theft”

A breach in your personal privacy protection could easily lead to hackers, online, and offline thieves stealing your identity.

The contents of this paper include:

~~~ 000 ~~~

This brief guide on protecting yourself, your family, and your friends from Identity Theft is offered at no charge by RichardPresents.com. It is a supplement to the wealth of information presented in the Free www.Firewalls-and-Virus-Protection.com website, Security Alert Newsletter, and Weblog.

The threat of Identity Loss exists on more than the Internet. The potential for the theft of our identities is everywhere around us. Following the advice in this guide will go a long way toward keeping your identity safe and secure.

.....*Richard Rossbauer*

IdentityTheft is a serious crime. People whose identities have been stolen can spend months or years - and their hard-earned money - cleaning up the mess thieves have made of their good name and credit record.

In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit.

Daily vigilance at home, in the work place and on the internet is necessary to reduce the risks of Identity Theft. Scams and fraud face all of us everywhere and there is the potential of being spied upon both off the internet and on. Every Family Member should be a participant in your personal security protection efforts.

Strategies To Protect Yourself Against Identity Theft

If you're a victim of identity theft you may spend months, even years, trying to repair a ruined credit history. A seriously damaged credit report can compromise your chances of getting a new job, a bank loan, insurance or even rental housing. It's even possible to be arrested for a crime you didn't commit if someone else has used your identity to break the law.

Unfortunately, many of the methods that thieves use to steal identities are beyond your control to guard against. Although it's rare, even store clerks have been known to use their position to pass along information to identity thieves.

There are some measures you can take, however, that will make it harder for a thief to steal your identity.

Protect Your Credit Card Number When Making Purchases

After you make a purchase and your credit or debit card has been swiped through a credit card terminal, check to make sure that the printed receipt hides all but the last 4 digits of your credit card account number (usually there will be Xs in place of the first 12 digits). Some terminals still print receipts that show all 16 digits of an account number, and may even include the expiration date as well.

After your card is swiped, you're permitted by law to hide the first 12 digits of your account number on the copy of the receipt that the vendor keeps. Use any marking pen that will do the job.

When you go to a restaurant, it's especially important to make sure that the first 12 digits of your credit card number are hidden on your receipt. You might be in the habit of signing it and then leaving the restaurant's copy on the table after your meal. An identity thief can easily steal the signed receipt before the waitperson comes back around to pick it up from the table. Don't take any chances.

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).

Do You Really Need To Give Your Social Security Number?

Another important way that you can guard against identity theft is to avoid giving out your social security number unless it's absolutely required. Although you need to share your social security number when you apply for credit or for a bank account, sometimes a store or an organization will want to use it as an ID number, simply to identify you within their system.

This is a common practice even though the law says that social security numbers aren't to be used as ID numbers. In these situations, use your judgment. There's usually an alternative if you ask.

Destroy Documents That Contain Sensitive Personal Information

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. Do not throw credit card statements, old credit cards or bank statements, etc. in the trash. That presents an easy way for someone going through the trash to steal your account information and use it as if they were you.

Buy a paper shredder and use it to destroy documents you're throwing away which contain personal information such as credit card numbers, social security numbers, phone numbers and dates of birth. Shredders that cross-cut are best.

This is important to do both at work and at home. Identity thieves aren't above going through your trash to find valuable personal information that can help them obtain credit in your name.

Some Other Common Sense Safety Steps

When 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. 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 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 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. This is often referred to as ‘phishing’.

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. This 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 shopping online, always use a secure browser and shop from a web site that offers secure transactions when shopping. 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.

Look for the ‘s’ in the web site ‘https’ addess code.

Keep your computer clean from spyware or Trojan programs that log keystroke information. Use virus protection software and spyware monitoring and removal software.

These programs should be updated regularly, and updates for your 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. Most browsers alert you when new updates are available. Don’t wait – update.

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. and the other major credit reporting organizations.

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.

Here are the important contact numbers:

Equifax: report fraud at 1-800-525-6285, order credit report: 1-800-685-1111
Experian: report fraud t 1-888-397-3742, order credit report: 1-888-397-3742
Trans Union: report fraud: 1-800-680-7289, order credit report: 800-888-4213
Federal Trade Commission ID Theft Hotline: 1-877-438-4338
Privacy Rights Clearing House: 1-619-298-3396
Identity Theft Resource Center, Email: voices123@att.net

If The Worst Happens

If you do become a victim of identity theft, take the following steps immediately:

Contact your credit card companies, close your accounts and ask to have new cards issued to you.

Place a fraud alert on your file with any one of the three major credit bureaus. The other two will be notified automatically.

File a police report. You may need it to show to creditors as proof of the crime.

File a complaint with the FTC, which maintains a database of identity theft cases used by law enforcement agencies for their investigations. You can do this online at http://www.consumer.gov/idtheft/

And be sure to call the Social Security Administration Fraud Line: 1-800-269-0271

Richard started his "Firewalls and Virus Protection" website and "Security Alert News Reporter" to help everyday Internet users navigate safely through the Cyber Space that has become a 'Cyber Jungle', loaded with ambushes and booby traps. He promotes his "Computer Security Awareness Campaign" thru his website at http://www.firewalls-and-virus-protection.com

---

Please help educate and protect the unwary by sharing this article. Reprint it if you have a newsletter, website or ezine. Copy or print it to give to your friends. It may be used at will so long as no edits or changes are made to the content and links, and the full attribute box is included. We'd appreciate a short note telling when and where you have posted it. Thank you....Richard (mailto:Richard@firewalls-and-virus-protection.com)

Whatever else you do with this guide, please include sharing it with the people you care about and wish to protect.

..... Richard Rossbauer