

Understanding and Avoiding Identity Theft

+++++

An article from Internet ScamBusters - <http://www.scambusters.org/>

This issue addresses what is probably one of the most frightening and least understood problems for many people today. Identity theft.

Identity theft was used by some of the terrorists on September 11.

This is a fairly complicated issue, so we're going to explain the basics here and give you pointers to some great resources you can use to learn more and to defend yourself.

The US Government defines it like this: "[I]dentity theft occurs when someone appropriates your personal information without your knowledge to commit fraud or theft."

To put that in more day-to-day terms, it works like this:

Someone gets your name, address, social security number and credit card or other information, and uses them to run up big bills, pretending they're actually you. They skip on the bills and leave you with ruined credit and collectors hounding you.

For those who have been there, it's a nightmare. The companies who made the loans often assume that you are the one who actually incurred the debt, and are trying to beat them out of their money. They can be very aggressive in their collection tactics. The stress, the paperwork, and the sleepless nights often take a bigger toll than even the debt.

The feeling of having been violated is something many victims say is the worst of all.

How Does This Happen?

It's easier than you might think, actually.

ANYONE who has access to the basic info needed to apply for credit, or even telephone or cell phone service, could potentially use that info to steal your identity. The clerk in the store where you applied for a credit card, your landlord, the cashier you handed your credit card to who asked for ID to verify your identity... Anyone at all.

As usual, life isn't like the movies. "The Net" made this sound like a high-tech risk, not something that could happen anywhere, at almost any time. It's true that there are high tech approaches that make things easier for some thieves, and we'll explain how to avoid them (or give you pointers on avoiding them), but don't stop there. Offline approaches are much more common.

Ever lose your wallet or your purse, or have them stolen? That's one common way the thieves get your information. Take a look through them right now, and see how much information about you is in them that a thief could use to successfully pretend they're you.

Scary, isn't it?

You can't prevent this with 100% certainty, but there are some things you can do to reduce your exposure.

First, only carry the info with you that you absolutely need for day-to-day dealings. For example, don't carry that gold card to do your grocery shopping. And don't put your social security number on your checks.

Keep an eye on your mail. Don't wait till the end of the day to pick it up. Better yet, get a mailbox that's harder for thieves to get into. And never allow your mail to build up while you're out of town. Stolen mail is one of the easiest ways to get someone's vital statistics.

Know your payment cycles on your credit cards. If the bill is late, call and ask why. It's not unusual for identity thieves to request a change of address for your credit card billing and run hefty charges up before you notice that you're not getting your monthly statements.

There are people who have legitimate reasons to ask for personal information. Employers, merchants, landlords, etc. Before you give out that information, know why they need it, and only give them what they actually need to complete the transaction.

Never give personal info to people who contact you out of the blue. A good example of this is an email spam that's going around now, with the return address AOLbilling@aol.com. The sender claims that your credit card info with AOL is out of date or lost, and that you need to email them details to avoid service interruptions.

This is one of the oldest scams going. Don't fall for it. No ISP (and very few legitimate companies) will ask you to send credit card info in an open email. When you get something like this, pick up the phone and call the number you got when you first dealt with the company and check it that way.

For more details on preventing identity theft, and dealing with it if you're already a victim, visit the US government's consumer site on the issue, at:

<http://www.consumer.gov/idtheft/>

Alternatively, you can download an excellent electronic book from the US Federal Trade Commission on the subject, entitled, "When Bad Things Happen to your Good Name" from:

<http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf>

These provide much more in-depth and comprehensive information than we could fit into this newsletter. You'll find them quite useful. And very eye opening.

How About Online?

The AOL Billing scam mentioned above is just one way this can happen online. Many of the others can be reduced by using the same common sense approach about where you give out information that is described above.

A few other things to do:

1. Watch out for merchants who offer prices that look too good to be true, and don't give you any offline way to contact them or verify their validity. If you know the merchant, you're probably safe, but if not - be careful.

This especially applies to offers you receive via spam. Remember: If it's spam, it's scam.

2. Don't post private information on discussion lists or forums, even if they're alleged to be private. You never know who's listening.

This may seem obvious, but you would be surprised at how much private information we've seen posted in places it should never be!

3. Keep your passwords off your computer, and always have different passwords for each site where you need them. Make sure they're not obvious words, strings of successive numbers, or anything else that would be remotely possible for someone to guess. Crackers frequently use programs that run what are called "dictionary attacks" on servers, looking for private info stored behind poor passwords.

A combination that includes both letters and numbers, and which is eight characters long, will make things much more secure.

4. Always run good, up-to-date anti-virus software and a personal firewall. There are ways that a program can be planted on your computer that will allow other people to take control of it, deleting data, running software, even downloading files from your machine. Including any personal information you may have stored there.

We mentioned an article a while back that explains this, along with a good overview of other security measures you should take to protect your personal data.

~~To get a copy, send any email to <mailto:security@talkbiz.com> It will arrive within minutes. It will be from Paul Myers, and the subject line will read "Data Security Article."~~

How Can I Know When I've Been Hit?

The only simple way is to track your credit history. Equifax in the US offers a service that will give you access to your personal credit file, and will email you within 24 hours of any change to that file. You can get the details at <https://www.econsumer.equifax.com>

We don't get any money for this mention, even if you use the service. It's just a very useful way to help protect yourself.

A True Story, From Someone Who's Been There

For information and tactics for dealing with this, from a real life victim of identity theft (she was roller-blading with her son when it happened), visit <http://stolen-identity.com/>

Be Careful Out There

The chances of your personally becoming a victim of identity theft are pretty small. But then, do statistics matter much when you become one?

It costs very little to protect yourself, and the peace of mind is well worth the effort. We encourage you to check out these resources and arm yourself against the people who would steal your name... and use it against you.

Be safe.