

## Identity Theft: Count The Ways

By: Daryl Campbell

I received an e-mail message from "Paypal" not too long ago. The e-mail stated that PayPal needed me to update and verify my security information for their database. I didn't. One of the sentences in the e-mail read:

"Complete the necessary verification tasks within 5 days, or your account might get temporarily suspended."

That didn't sound like the PayPal I've been doing business with for several years. The grammar of "your account might get temporarily suspended" raised an alarm bell. Also the logo while quite professional looked odd.

But the obvious giveaway was knowing Paypal would never contact me at an e-mail address I never gave them. I could have become a victim of a technique called phishing. Just another form of Identity theft.

The effort criminals put into stealing your identity staggers the imagination.

With Phishing also called brand spoofing, criminals set up phony but legitimate looking websites then spam you with e-mail like the one described above in the hopes of catching a percentage of Internet users. No reputable business will ever ask for your personal information via e-mail information.

Phishing just became a parent to a newborn child called "pharming". Hackers plant phony information into DNS servers. This allows them to match domain names with the database of IP addresses maintained by various web hosting companies. In other words you type in a web address press enter and get rerouted to bogus websites where identity thieves are waiting to grab any of your information.

2003 saw identity thieves target Ebay account holders, this year it's Paypal's turn but any company with a database of information remains a target.

Choicepoint a veritable clearinghouse for the insurance industry finds themselves trying to explain how identity thieves tapped into their system to defraud 145,000 customers across the U.S. Investigators in California place that number closer to a half a million.

The hackers apparently used previously stolen identities to apply for and receive business licenses then bought information from ChoicePoint whose database totals 19 billion public records.

The FTC estimates that this year alone identity theft will cost the business community 4.2 billion dollars and 8 billion by the end of 2006.

Easy access to computers provide more chances for identity theft but the majority of cases according to the Better Business Bureau happen offline. Mail fraud public spying known as "shoulder or telephone scams that target the elderly surfing" contribute greatly to this epidemic.

Unfortunately senior citizens face another threat known as the "sweetheart scam" in which a criminal offers to run errands or do chores around the house for the express purpose of taking control of the victim's finances.

Taking control of someone's finances can also happen in a restaurant, department store or any legitimate place of business. When a clerk swipes your card twice without your knowledge then stores the information for later use this is known as skimming. Often the clerk will make a duplicate card with your info to go on a buying spree or sell it on the black market. The illegal selling of credit card information as you might have already guessed is big business.

Identity theft has forced many financial institutions to revamp their ATM's due to criminal rigging. A person uses the ATM but after putting in the pin# the machine keeps the card. Usually when the person goes to report it, the thief strikes, taking card, pin # and most importantly the victim's identity.

The methods of madness can include something simple like going thru your trash known as dumpster diving or an elaborate hoax similar to the one reported by the Associated Press.

A family in the Pacific Northwest posed as tax preparers and used stolen identities to go on buying sprees across several states that included million dollar homes and luxury vehicles. According to authorities, since the thieves stole the social security # of children as well as adults, the damage won't be fully known until these young people start applying for credit later on.

Law Enforcement officials believe the next step with this criminal outfit involved applying for health care positions. Hospitals and doctor offices provide a wealth of personal information. Perfect for Identity thieves

These methods along with old fashioned robbery show why identity theft according to the Department of Justice maintains it's ranking as the number one and fastest growing crime in the US for 5 consecutive years. Unfortunately, it will maintain that status for the near future.

### About The Author:

Daryl Campbell owns and operates <http://winthemarket.com>. He has written a 4 part report on Identity theft. Grab your free copy at <http://digbig.com/4djxq>. Learn more about this worldwide epidemic and how you can protect yourself. <http://digbig.com/4djxq>

Article Source: [www.isnare.com](http://www.isnare.com)