



## Identifying Thieves through IDs

The most explicit threat to privacy nowadays is identity theft. Incidences have rapidly grown in just a few years as the means to accessing data becomes easier thanks to advancements in technology. The US alone has suffered billions of dollars worth of losses from credit card and insurance claims fraud. We all know we are potential victims to this crime. We can't be too careful with using our credit cards, email accounts and websites. We can't be too sure about trusting people, health care providers and companies with our personal information. Who are these people whom we are so afraid of anyway? What are they like and how do they operate?

Hackers and spammers are the first type of people that we suspect. Aside from online databases, and company servers, they are capable of infiltrating email addresses, not just for the enjoyment of stalking, but to harvest personal information about you. Profitable information is more attractive than your romances after all. Hackers with the intention of (1) [stealing your identity](#) can infiltrate your account and gather vital information about yourself through online billing statements, transactions with companies, learn about your contacts and your relationship with them, and finally ban you from using your account again. They then use your identity to ask money from your friends and people you trust, use the information they have gathered to open new accounts, claim insurance, use your credit account, and many more nasty things. Other than emails, they can also use programs such as keyloggers to harvest information from frequently used computers. This is why people should always be careful with storing and sending sensitive information through the web and be wary of public access computers.

Organized criminals operate in more complex ways. They create the means to conspire against the victim, and this involves a lot of money. Big business as it is called. One way to cash in on the booming identity theft business is by taking over some businesses that handle private data such as small clinics and insurance providers. They gather all the clients' data and use them in a lot of different ways. If they can't afford to take over businesses, they hire people to gather it for them. Insiders that have access to tons of data from government offices, to insurance companies, to hospitals are able to provide information to the crime rings for a price. Why do these people invest on scheming for new ways to harvest data? Unlike in dealing drugs, the danger involved in the identity theft business aren't as bad as facing guns, bombs and assassins. The penalties if they get caught are also lesser in gravity. Drug syndicates and other illegal trade organizations are now shifting their focus on identity theft as the new business venture for the information technology age.

Many recent studies show a more disturbing profile for identity thieves. In most cases of fraudulent use of credit cards and other services, the perpetrators are either relatives or people we know very well. These are the people who know our habits and personal details very well. They are people we trust well enough to have access to sensitive documents, and they would only need little effort at obtaining enough data to start using them maliciously. These are the cases that are rarely reported since only a few would want one of their sobbing relatives or friends jailed. Truly, you can never be too sure about trusting people with your secrets, more so, never trust a link that was sent to you via email or instant message as well.

If you are a web user and you were prompted to ask for your password, personal information online, make sure that you're dealing with legit businesses or legal personnel. For the same reasons, you may have heard largely of Parental Controls, spam filters, Anti Virus systems and the like when surfing the net. These are some of the programs that received the buy-ins of the web users because of the need to secure accounts and personal information. Remember, you would not know who's watching you from a distance. When you were given the opportunity to ID these thieves, take a greater action through proactive involvement on how to put these thieves to jail just like what happened in (2) [Virginia in 2004](#) and when a (3) [teen hacker was put to jail in 2001](#).



**Fluxcard.com Fake ID Articles**  
**Original Research Articles © Fluxcard.com 2007**

With so many incidents of youth delinquents happening all over the globe, it is but logical to think how could there be ways in protecting one's identity, more so, protecting the right to privacy? This quest may appear to be a really tough challenge for all concerned but it is not yet late to bring privacy rights to its position and protect it.

- (1) [http://blog.washingtonpost.com/securityfix/2006/11/boarding\\_pass\\_hacker\\_breaks\\_si.html](http://blog.washingtonpost.com/securityfix/2006/11/boarding_pass_hacker_breaks_si.html)
- (2) <http://www.pcworld.com/article/id,118493-page,1/article.html>
- (3) <http://news.bbc.co.uk/1/hi/wales/1424937.stm>