

Net Threats – What’s the Big Deal about ID?

This is the first in a series on the serious matter of Internet Threats. These “threats” (the risk of having your Identification stolen and abused) keeps the act of going online a risky and ever growing, dangerous venture. We want to make you aware of the danger and teach you to protect your computer and your identification.

According to a recent Consumer Reports (CR) article (September 2007):

- In 2006, identity theft cost consumers and businesses \$49.3 billion,
- Your chances of becoming a ‘cybervictim’ are about 1 in 4,
- Approximately 8% of all CR survey respondents (estimated 1 million people) are still falling victim to phishing scams (bogus e-mails and web sites that ask for disclosure of your financial information),
- 38% of all CR respondents reported a computer-virus infection in the last 2 years – these infections cause roughly 1.8 million households to replace their PC’s,
- 34% reported a spyware infection in the last 6 months – causing approximately 850,000 households to replace their computers,

These modern day thieves, who steal your ID and your money, have their own extensive network of underworld connections, websites and chat rooms. They brag about their ‘accomplishments’, train each other on how to be successfully fraudulent, sell stolen information, obtain tools for making credit cards, purchase high tech surveillance equipment to record ATM card numbers and their associated PINs, and more. Despite extensive efforts by law enforcement, the advancement of sophisticated security software that is available to the consumer, and the high level of visibility of these crimes, these *Internet Threats* remain potent. In short, the criminals have become more sophisticated than law enforcement. The average internet user MUST become more aware of these threats, of the methods employed to obtain ID information, and what can be done to minimize the chances of becoming a victim.

Victims face a long, stressful, and tedious process. Based on the type and extensiveness of the ID theft crime, there may be a police report, contacts to banks, credit card companies and the three credit reporting agencies, shutting down various accounts, and perhaps putting a block on credit uses. You may be contacted by collection agencies and lawyers demanding payment for things you never ordered.

You are guilty until you prove your innocence. Don’t be surprised if Homeland Security is contacted by some reporting agency about your case. That is the unfortunate extent of the seriousness of these assaults against consumers.

There are several good links available to victims of ID Theft, which give you tools, forms, and direction on how to proceed through the process of reclaiming your identity. They are listed below:

- <http://www.privacyrights.org/fs/fs17a.htm>
- <http://www.usdoj.gov/criminal/fraud/websites/idtheft.html#whatifvictim>
- <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>
- [https://rn.ftc.gov/pls/dod/widtpub\\$.startup?Z_ORG_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpub$.startup?Z_ORG_CODE=PU03)
- <http://www.ojp.usdoj.gov/ovc/help/it.htm>

Of course, the best offense against these threats to our identity is a good defense. In the next article, we will discuss how to stay safe while on-line.