

The Inside Secret Of Identity Theft And What You Must Do To Protect Yourself

Article by: Henry Tom

Identity theft is the use of other's personal information or identification without permission.

Under the **Fair Credit Reporting Act**, identity theft is defined as *"the use or attempted use of an account or identifying information without the owner's permission."*

The **1998 Identity Theft and Assumption Deterrence Act** also describes "identity theft" as *"knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."*

Information Privacy & Protection

Identity theft isn't about "stealing identities."

Identity theft comes down to information – the lack of protection, privacy and checking of that information.

Physical identification is just an added layer of convenience and security around information. A blank plastic card, device, object, or sheet of paper has no identification value by itself. Meaningful information about the issuer and holder give value to the identification.

Personal information eventually must be secured to prevent identity theft.

In the perfect world, this security would also mean ensuring privacy, and proving rightful use. If companies made 100% sure the people they're doing business with are who they claim to be, identity theft wouldn't exist.

Identity Theft's Major Cause - Poor Information Protection

Given personal information should be locked up and kept safe, why is identity theft running rampant?

You'd figure business and government organizations would give top priority to protecting and checking personal information.

That's not always the case. Monthly - and increasingly frequent news reports of massive security breaches prove this point.

According to Privacy Rights Clearinghouse, 299 business and government security breaches exposed over 93 million personal records between February 15, 2005 and September 7, 2006. That's one security breach reported every two days!

Many of these records are enough for successful identity theft.

So why so many security breaches today?

More organizations than before have reported security breaches due to a few new state laws. And it's getting worse.

The recent wave of security breaches was only the tip the iceberg. Not all organizations and companies need to report security breaches. Besides, many don't even know it's happened.

The reality is the situation's far worse than the exposed 93 million personal records. It's hard to tell how bad it was before, and how deep it goes today.

No one's talking unless they're forced.

The Secret of Behind Information Privacy & Protection Today

Here lies the secret seasoned privacy and security professionals know, but remain powerless over.

Personal information security and privacy are not top priorities for government or business.

Why?

Security And Privacy Take Backseat To Business Profit

Businesses exist to make a profit. Yes, businesses exist to satisfy customers too, but only as a means to turn a profit.

Security and privacy safeguards are costs to a business. They cut away profits. The thinking is don't spend on security unless you have to. Often, it's based on "best judgment" – not by law.

Even if security were a high priority for businesses, security spending could go on forever.

In such situations, accepting risk overrides spending. Business managers decide between protecting personal information and producing profits. Banks fit in this category, but even banks have reported security breaches.

Security And Privacy Take Backseat To Government Optics

Governments work different.

Balancing budgets, spending and good appearances for voter approval drive priorities.

Security and privacy are not high priorities unless the public sees symptoms. The thinking in government often is -- it's not a problem if we don't know about it, and the public doesn't know either. What matters is doing what looks good.

Anyway, there's nothing wrong with making a profit or balancing budgets.

The problem comes when businesses sacrifice security and privacy for profit; and governments neglect security and privacy for vote buying initiatives.

Recent security breach reports confirm this is the case for many business and government organizations.

Consumer Choose Lower Cost And Convenience Over Security

The issues also get more complex with consumer and public choice. In other words, consumers and the public choose less security.

Consumers won't pay extra for security - unless they're buying security as the product or service i.e. an alarm system, a bodyguard, a burglar safe, etc.

Consumers also prefer convenience over security. They want it now, and they want it to be as easy as possible.

Businesses won't put in security measures to inconvenience customers - unless its competitors do too, or everyone's forced to do so.

Consumers expect businesses to have strong security anyway. Unless consumers decide with where they spend their money, businesses will put in just enough security to manage losses – at best.

With the number of security breaches reports so far, businesses appear they don't know they have inadequate security; or they're aware, yet they've chosen to gamble with personal information instead.

The public also won't stomach paying large sums of tax dollars for government security - especially when it's hard to prove positive results. The public also doesn't think highly of heavy-handed government security.

No One To Pay The Price To Protect Personal Information

The issues get even more complex, but the main point is no one wants to pay the price to protect personal information.

Everyone wants the benefits of security and privacy to stop problems like identity theft; but, no one wants to pay the costs, or bear the inconvenience that go with increased security for privacy.

The reality is the security problems won't go away overnight.

In fact, new laws forcing more businesses and governments to report security breaches will reveal a worse landscape. Even then, the full extent of the problem will remain hidden.

So who's to stand up for change? Government, businesses, consumers, the voting public, or all of the above?

As it stands, it's none of the above. Perhaps the unveiling of more security breaches might propel change. There must be a tipping point when everyone says "enough!"

What To Do Now

Given the current state, it's only time before you'll become an identity theft victim.

You should take all measures to protect yourself from the threats.

You can lower your risk by keeping your personal information private as much as possible. In addition, constantly monitor for signs of identity theft, and educate yourself on this subject so you can respond as needed. Last, you can insure against identity theft.

You unfortunately don't live in a perfect world. You live in a complex world, where the masses make imperfect decisions.

All you can do is protect yourself the best you can as an individual – and promote the message for change.

This article may be reproduced in printed or web format, provided the resource box below is included. Henry Tom is a widely known information security and privacy professional based out of Toronto, Ontario, Canada.

He's worked in government communication security, and banking information security for nearly a decade. During the time in banking, he worked on national and international security projects for banking crime prevention and investigations. Over the past six years, he's specialized in digital identity security, and secure identification for the government. He's also written three ebooks - two on identity theft for industry experts and trainers.

Find out at his web sites how you can keep from becoming an identity theft victim: <http://Protect-My-Info.com> & <http://Inside-Identity-Theft.com>