

Preventing ID Theft

Preventing ID Theft: The Basics

Will you be a victim of Violent Crime? The odds are 1 in 5,000

Heart disease? 1 in 2,600

Car accident? 1 in 130

However, the odds of being a victim of identity theft are only 1 in 23.

Your chance of losing important data is 1 in 2.

What is Identity Theft?

According to the United States Department of Justice, the terms identity theft and identity fraud “refer to all types of crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically for economic gain.”

ID Theft leaves devastation in its wake: ruined credit history, and the difficult, time-consuming task of proving that you did not rack up the charges made in your name. The nonprofit Identity Theft Resource Center estimates the average victim spends 600 hours trying to clear up credit problems.

The figures are only going to escalate in the coming years. Identity thieves make a lot of money and they are rarely caught. Every day, criminals are finding new ways to steal financial identities.

How widespread is Identity Theft?

According to the Federal Trade Commission, nearly 10 million people fall victim to identity theft annually, costing consumers \$5 billion in out-of-pocket losses. The cost to businesses is estimated to be \$48 billion.

Data Loss

A lot of personal data that has been compromised has been “lost” rather than stolen. Many of the nation’s top data handlers have gaping loopholes in their security systems that enable thieves to harvest the financial identities of millions of people. Once lost, there is no telling what could become of this sensitive data.

In cases like this, prevention strategies are of little or no help. Identity protection is beyond the control of the individual. ID theft insurance is the only remedy.

Some examples of data loss that occurred in 2005:

- **CitiFinancial, the consumer financial division of Citigroup notified customers that computer tapes containing their SSNs and account data were apparently lost in transit some time between May 2 and May 20. 3.9 million customers affected.**
- **Bank of America notified customers that computer data tapes containing personal information on federal employees, including some members of the U.S. Senate, were lost. 1.2 million customers affected.**
- **Ameritrade, the discount broker reported it notified current and former customers that it lost a backup computer tape containing their personal information. 200,000 customers affected.**
- **Time Warner announced that data on current and former employees stored on computer back-up tapes was lost by an outside storage company. 600,000 individuals affected.**

Passwords

One of the easiest protections against ID theft is a “strong” password. A strong password is one that is difficult to figure out and impossible to guess. Never use birthdays, phone numbers, or anniversaries. The most common passwords are addresses, parts of Social Security numbers and pets’ names.

Strong passwords should have ten characters including numbers. Uppercase and lowercase letters add additional strength.

Here is a good way to generate a very strong password that you can remember:

Make up a sentence, with numbers and proper nouns in it, that has some basis in reality for you. Take the first letter of each word, capitalize proper nouns and use some symbols.

For example – C&Ph2dnS&K is a strong password that may seem difficult to remember. It comes from “Chris and Pat have two dogs named Spot and Killer.” For Chris, this is a very easy password.

- **Type your login and password every time you use it. Do not let your computer automatically fill in or save your passwords. If your password fills in automatically, identity thieves could have easy access to all your information.**
- **Never give out your passwords to friends, co-workers or family. Often, identity thieves are people known to the victims.**
- **If you write down your password, don't keep it anywhere near your computer.**
- **Use different passwords in different environments. For example, use different passwords at home and at work.**
- **It is a good idea to change your password every three months.**

Common Behaviors to Avoid

- **Never carry your Social Security number with you.**
- **Don't leave mail –especially bills, business correspondence with account numbers, financial data and personal information- in unlocked boxes where a “flag” indicates to the letter carrier that there is mail inside to be picked up.**
- **Release your personal data only to agencies that require it for action you have initiated.**
- **Never give credit card numbers or personal data to phone callers if you did not initiate the call or ask to be called.**
- **Never provide personal data on an unsecured Web site.**

- **If you are notified by mail or phone that you received a prize, you should not have to pay any fees or provide any information to claim it, if it is a valid offer.**

Fight ID Theft with iS3 Products

iS3 anti-Spyware solutions –STOPzilla provides optimal protection from Spyware and Phishing attacks. It enables you to maintain your privacy and security by clearing cookies, erasing your surfing history and learning about how to avoid online fraud wherever possible. You can download the free trial version of STOPzilla at: <http://www.stopzilla.com>.

The ZILLAbar is a free anti-Phishing toolbar that provides protection from Phishing attacks and delivers high quality search results. You can download the free trial version of STOPzilla at: <http://www.zillabar.com>.

All iS3 products are designed to deliver the highest standard of protection available.