



Multi-State Information Sharing & Analysis Center (MS-ISAC)

Monthly Cyber Security Tips

NEWSLETTER

DECEMBER 2006

Volume 1, Issue 7

Preventing and Responding to Identity Theft

From the Desk of William F. Pelgrin, Chair

We each have a responsibility to protect data in our care – whether data is our own personal info or that of an organization. When we understand and employ good security procedures, we can make great strides in preventing the theft and misuse of confidential data. We each have an opportunity to help our fellow citizens, customers, and co-workers by ensuring any confidential data that we store, maintain, or transmit is not compromised. By following your organization's security policies and being mindful of the risks and threats to confidential data, we can each make a positive difference in reducing data theft and helping prevent identify theft.

Below are some helpful hints from US-CERT on how you can protect your own personal information.

Identity Theft

Identity theft, or identity fraud, is a crime that can have substantial financial and emotional consequences. Take precautions with personal information; and if you become a victim, act immediately to minimize the damage.

Is identity theft just a problem for people who submit information online?

You can be a victim of identity theft even if you never use a computer. Malicious people may be able to obtain personal information (such as credit card numbers, phone numbers, account numbers, and addresses) by stealing your wallet, overhearing a phone conversation, rummaging through your trash (a practice known as dumpster diving), or picking up a receipt at a restaurant that has your account number on it. If a thief has enough information, he or she may be able to impersonate you to purchase items, open new accounts, or apply for loans.

The Internet has made it easier for thieves to obtain personal and financial data. Most companies and other institutions store information about their clients in databases; if a thief can access that database, he or she can obtain information about many people at once rather than focus on one person at a time. The Internet has also made it easier for thieves to sell or trade the information, making it more difficult for law enforcement to identify and apprehend the criminals.

How are victims of online identity theft chosen?

Identity theft is usually a crime of opportunity, so you may be victimized simply because your information is available. Thieves may target customers of certain companies for a variety of reasons: a company database is easily accessible, the demographics of the customers are appealing, there is a market for specific information, etc. If your information is stored in a database that is compromised, you may become a victim of identity theft.

Are there ways to avoid being a victim?

Unfortunately, there is no way to guarantee that you will not be a victim of online identity theft. However, there are ways to minimize your risk:

- **Do business with reputable companies** - Before providing any personal or financial information, make sure that you are interacting with a reputable, established company. Some attackers may try to trick you by creating malicious web sites that appear to be legitimate, so you should verify the legitimacy before supplying any information (see [Avoiding Social Engineering and Phishing Attacks](#) and [Understanding Web Site Certificates](#) for more information).
- **Take advantage of security features** - Passwords and other security features add layers of protection if used appropriately (see [Choosing and Protecting Passwords](#) and [Supplementing Passwords](#) for more information).
- **Check privacy policies** - Take precautions when providing information, and make sure to check published privacy policies to see how a company will use or distribute your information (see [Protecting Your Privacy](#) and [How Anonymous Are You?](#) for more information). Many companies allow customers to request that their information not be shared with other companies; you should be able to locate the details in your account literature or by contacting the company directly.
- **Be careful what information you publicize** - Attackers may be able to piece together information from a variety of sources. Avoid posting personal data in public forums (see [Guidelines for Publishing Information Online](#) for more information).
- **Use and maintain anti-virus software and a firewall** - Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall (see [Understanding Anti-Virus Software](#) and [Understanding Firewalls](#) for more information). Make sure to keep your virus definitions up to date.
- **Be aware of your account activity** - Pay attention to your statements, and check your credit report yearly. You are entitled to a free copy of your credit report from each of the main credit reporting companies once every twelve months (see [AnnualCreditReport.com](#) for more information).

How do you know if your identity has been stolen?

Companies have different policies for notifying customers when they discover that someone has accessed a customer database. However, you should be aware of changes in your normal account activity. The following are examples of changes that could indicate that someone has accessed your information:

- unusual or unexplainable charges on your bills
- phone calls or bills for accounts, products, or services that you do not have
- failure to receive regular bills or mail
- new, strange accounts appearing on your credit report

- unexpected denial of your credit card

What can you do if you think, or know, that your identity has been stolen?

Recovering from identity theft can be a long, stressful, and potentially costly process. Many credit card companies have adopted policies that try to minimize the amount of money you are liable for, but the implications can extend beyond your existing accounts. To minimize the extent of the damage, take action as soon as possible:

- **Contact companies, including banks, where you have accounts** - Inform the companies where you have accounts that someone may be using your identity, and find out if there have been any unauthorized transactions. Close accounts so that future charges are denied. In addition to calling the company, send a letter so there is a record of the problem.
- **Contact the main credit reporting companies (Equifax, Experian, TransUnion)** - Check your credit report to see if there has been unexpected or unauthorized activity. Have a fraud alerts placed on your credit reports to prevent new accounts being opened without verification.
- **File a report** - File a report with the local police so there is an official record of the incident. You can also file a complaint with the Federal Trade Commission.
- **Consider other information that may be at risk** - Depending what information was stolen, you may need to contact other agencies; for example, if a thief has access to your Social Security number, contact the Social Security Administration. You should also contact the Department of Motor Vehicles if your driver's license or car registration has been stolen.

Copyright Carnegie Mellon University, Produced by US-CERT

The following sites offer guidance for both preventing and recovering from identity theft:

- Federal Trade Commission <http://www.consumer.gov/idtheft/> and <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm>
- United States Department of Justice - <http://www.usdoj.gov/criminal/fraud/idtheft.html>
- Social Security Administration - <http://www.ssa.gov/pubs/idtheft.htm>
- OnGuard Online - <http://www.onguardonline.gov/idtheft.html>

In addition, OnGuard Online has created a short quiz called “ID Theft FaceOff!” to help you remember how to protect your identity: http://onguardonline.gov/quiz/idtheft_quiz.html

Brought to you by:



MS-ISAC

<http://www.msisac.org>



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

<http://www.us-cert.gov/>