

# nbc5i.com

## Protect Yourself From Fastest Growing Crime: ID Theft

### *Millions Find Themselves In Nightmare Situations Because Of Stolen Identities*

*Brent Suyama, Staff Writer*

UPDATED: 7:03 am CST November 27, 2006

About 19 people a minute become new victims of identity theft, according to the Identity Theft Resource Center.

ID theft is the fastest-growing crime in the United States, according to authorities. About 10 million people a year find themselves in trouble involving their identity.

#### My Money

Protect Yourself | Fraud Myths | Prevention Tips

One complaint filed with the Federal Trade Commission sums up the frustration that victims face when their identity is stolen:

"I first was notified that someone had used my Social Security number for their taxes in February 2004. I also found out that this person opened a checking account, cable and utility accounts, and a cell phone account in my name. I'm still trying to clear up everything and just received my income tax refund after waiting four to five months. Trying to work and get all this cleared up is very stressful."

Los Angeles and New York City recorded the highest number of complaints in 2005, according to FTC documents.

In many cases, thieves who take your personal data have a job where they have access to the information. Other sources include bribing someone who has the access, stealing the data from a computer or even a laptop, stealing mail, wallets or bank records, searching trash and one of the most recent trends: phishing.

Phishing is when a fraudulent company or person steals your information from you by posing as a legitimate company that has a problem with your account. The request for your information usually comes in an e-mail or phone request.

One of the main tools of identity thieves is your Social Security number. That nine-digit code can give them access to tax records, allow them to open bank and credit card accounts, buy a car or even give your name in an arrest by authorities.

Many government agencies have eliminated printing people's Social Security numbers on documents or IDs. Banks no longer suggest customers place their Social Security numbers on their checks.

Here are a few tips on how to protect yourself from becoming a victim.

- Don't carry your Social Security card. Leave it in a safe place.
- Order copies of your credit report. You are entitled to a free report every 12 months.

More



Kaadaa/Stock Illustration Source/Getty Images

- Shred documents that have personal data, such as bank account statements and credit card applications.
- Place your outgoing mail in postal collection boxes instead of your home mailbox.

## **Internet Crime Grows Along With Web Explosion**

We have become heavily reliant on the Internet. What did we do before the Web?

We pay bills, manage accounts and shop online. However, that gives us another layer of vulnerability of which thieves are quick to take advantage.

That computer in your home or office can be fortified with a few easy programs that help keep intruders at bay. Adding a firewall, a program that keeps invaders from gaining access to your computer without your approval, can be one of the easiest moves. If you run Windows XP, you can turn it on in your settings. There are also programs you can buy at computer stores that do the same.

Another smart thing to do is keep updated virus protection on your computer. It can keep hackers from coming into your computer through weaknesses.

And get rid of spyware. No, we're not talking the James Bond type of spying. Hackers use programs called spyware to look for your personal data in your computer or track the keystrokes you make on your keyboard. That could give them access to your passwords. There are programs on the market that can help block or alert you when spyware is trying to download into your computer.

Avoid keeping your private information on your computer. This may seem like a no-brainer, but do not store your Social Security number, birth dates, account numbers or other private information on your hard drive. If you have to, make sure you have the anti-spyware programs and other protection that lowers your risk of having your data stolen and require difficult passwords to access the information.

## **Financial Companies Target Theft Prevention, Fraud**

Companies that deal with finances and sales find themselves on the front lines of protection against theft.

Credit card giant Visa said it has taken steps to stay ahead of criminals.

"One of the latest innovations we have put into the marketplace is something called Advanced Authorization. It looks at every single transaction in the Visa system and scores it in real time for its potential to be fraud," Vice President of Visa Corporate Communications Rosetta Jones said. "With this new technology, we're able to prevent fraud right at the checkout line."

The company deals with millions of transactions each day. The new program keeps track of your accounts and analyzes your spending habits. That helps make Visa aware of unusual activity on accounts.

"We're looking for unusual patterns," Jones said. "We're looking for systemwide attacks. You might be one card account in an attack that's broader than just that individual. So we are looking both at the card level and across the entire system to look for these fraud patterns and trends."

Consumers should know that they -- the consumers -- are not liable for fraudulent credit problems.

Credit card companies also look for duplicate accounts that may have been opened using your identity by an ID thief.

One of the companies that is under attack constantly is eBay and its subsidiary PayPal. PayPal handles financial transactions over the Internet and is the preferred way of payment on eBay.

PayPal has 123 million customers with accounts. Its parent company eBay has 212 million people with accounts worldwide.

The company focuses on educating customers about protecting their accounts and their password.

"The thing about the password that I think is key and a lot of people miss is that nobody knows your password except for you," PayPal spokeswoman Amanda Pires said. "The only way that someone can get your password is if you give it out. So actually, the power is in your hands."

Pires warned that customers should not give out their information or make passwords easy to guess.

The company echoes some of the things that Visa and other financial companies do. Its fraud department tracks spending habits of members.

eBay and PayPal members often find phishing e-mails that lead them to "spoof" sites, or sites that are designed to look like a legitimate sites, but are there to gather personal information.

One tool that eBay has created is a toolbar that users can download. The toolbar lights up red when a member logs into a site that is made to look like eBay or PayPal. When a member is on a legitimate site, the bar turns green.

The company has developed relationships with Internet service providers to target the fraudulent sites. ebay's fraud department contacts the ISPs to shut down the illegal sites.

Pires said that once a fraud site is found, the company works to get the site shut down as soon as possible.

"We also work closely with law enforcement and we have been successful in tracking down some of these bad guys who are sending these fake e-mails and actually making arrests, especially in countries in Eastern Europe like Romania," Pires said.

There are cases where people's accounts have been wiped out after having their password stolen or having given out the information. PayPal will reimburse the funds, but Pires warns that keeping track of your password will keep from having your account taken over or funds stolen.

"Nobody likes (having their identity stolen). Of course we don't want that to happen to our customers, so what we're really focusing on is education and prevention," Pires said.

### **Tips: What To Do When Your Identity Is Stolen**

The Federal Trade Commission offers four tips on what to do if you believe your identity has been stolen.

1. Contact the fraud departments of any one of the three consumer reporting companies to place a fraud alert on your credit report.
2. Close the accounts that you know or believe have been tampered with or opened fraudulently.
3. File a report with your local police or the police in the community where the identity theft took place.
4. File your complaint with the FTC.

### **More Resources:**

FTC Online Complaint form

The FTC and others suggest getting credit reports as part of protecting and steps once you believe you're a victim:

**Equifax:** 1-800-525-6285; P.O. Box 740241, Atlanta, GA 30374-0241

**Experian:** 1-888-EXPERIAN (397-3742); P.O. Box 9532, Allen, TX 75013

**TransUnion:** 1-800-680-7289; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

*Distributed by Internet Broadcasting. This material may not be published, broadcast, rewritten or redistributed.*