



internet help site

HEALTH ADVICE FOR YOUR COMPUTER



IDENTITY THEFT

What's Identity Theft?

Simply, it's assuming (stealing) someone's "real world" identity for the purpose of committing fraud and/or crime. If they get their hands on enough information, they are able to:

- open up fraudulent credit card accounts
- apply for loans
- attempt to secure other property using the stolen identity
- use your name to secure employment and to divert taxes

By far the scariest aspect is the connection to major crime. Identities are created and sold on a regular basis. Crime and drug syndicates, tax cheats, illegal immigrants, foreign nationals, fugitives and terrorists...they're all looking for a new "face". That face could be yours!

Someone could be using ***your*** name to commit crimes, and guess what happens next? The Police or Federal government agents are coming after **YOU!**

The Federal Trade Commission released a survey in September of 2003 showing that 27.3 million Americans have been victims of identity theft in the last five years, including 9.9 million people in the last year alone. That equates to approximately 4.6% of the U.S. population! According to the FTC survey, 2002 identity theft losses to businesses and financial institutions totaled nearly \$48 billion and consumer victims reported \$5 billion in out-of-pocket expenses.

This is a growing problem. How does this happen? Read on...

Take note!

One of the latest and **most dangerous threats to privacy** in today's high tech age lies in the potential use of spyware.

Spyware can be used to gather all types of confidential information and in most cases the user has no idea that the information is being taken. Everything you do online is being monitored and is at risk, including usernames, passwords, online shopping purchases and e-mail or chat correspondence.

Criminals are rubbing their hands with glee. This type of information is a real treasure trove and is just what they need to initiate identity fraud.

Many of today's most popular spyware applications are able to execute via remote installation; i.e.; they don't need physical access to the machine. These programs are sold every day to consumers who want to monitor their kids, employees, or spouse.

Beware. Spyware can be used to illegally obtain YOUR personal information and use it to create false identities or to strip bank accounts. It is being done as we speak. Take action to protect yourself!

Public Terminals... Are you as safe as you think?

Check this out. You won't believe it!

For over a year, people who used Internet terminals at Kinko's stores in New York were being monitored. In at least a dozen Kinko's stores, spyware that logged keystrokes had been covertly installed. Everything the users typed, including their passwords to financial institutions had been recorded. He captured more than four hundred user names and passwords, using them to access and even open bank accounts online.

This is a real world example of how spyware can be used to steal someone's identity. It is logical to conclude that more of this type of ID theft will occur because it is relatively easy to execute.

A thief doesn't even have to be technically skilled to install a commercial key logger and to retrieve your personal information. Once installed, the thief can have information e-mailed back to them or the software will open up a "backdoor" where the spy can log into the machine and retrieve keystroke or snapshot logs.

Exercise caution when using public computer terminals. Because you're in an open and unsecured computing environment, you're at risk and vulnerable. Do not send or retrieve any personal or sensitive information. Do this on your own secured PC at home.

Protect your personal information

Carry as little in your wallet or purse as possible. You should not carry around bank account numbers; personal identification numbers (PINs), passwords, passports, birth certificates, Social Security cards, credit cards, cheque books, ATM cards, etc. Especially not all of them in the same place, at the same time. Leave them at home, preferably in a safe! Take only what you need. Consider separating your wallet from your bag.

Check up on your personal credit report

It's important to check your credit report on a regular basis. Apart from the fact that you need and should know what's in it, you may well find some discrepancies. The question is, who put them there! It could be an honest mistake or you may have been targeted for fraudulent activity. Check it out. You might find:

- a change of address you did not initiate
- financial accounts for which you did not apply
- incorrect personal information or credit history

Speak to the relevant parties and request that your records be rectified.

Note

A study by the FTC on identity theft found that 52% of all ID theft victims found out by monitoring their accounts.

After applying for a loan, credit card, rental or anything else that requires a credit report, request that your Social Security or Tax number on the application be truncated (x'ing out key numbers) or completely deleted and your original credit report be shredded or returned to you after a decision has been made. They only need your credit score to justify a decision.

Card use

Watch your monthly billing statements for errors or unusual activity.

If your card is swiped by those manual machines that use a carbon copy (yes, they still use them, especially when computers crash), ask for the carbon copy as well as your receipt. Hundreds of these carbon copies sit in bins waiting to be disposed of and are easily picked up by thieves. That imprint has all of your details on it.

Be aware of unscrupulous operators in places such as shops, petrol stations and markets. Watch exactly where your credit card goes! If it goes under the counter or out the back, there's a possibility that your card is being scanned, imprinted, copied or even your account hacked. Keep your eyes open.

There have been instances of ATMs being hijacked by thieves and even hidden cameras being set up to monitor your keystrokes and hopefully get your PIN number. Again, keep your eyes open as to what is going on around you.

Destroy any pre-approved credit card offers. Again this has all of your info on it. Consider opting out of any offers.

If your statement is late, call the bank to check if there have been any changes to your details. Your mail might have been intercepted.

Never give out credit card or personal information over the phone unless you initiated the call.

There have been very clever scams and sales pitches that make you reveal your personal details to telemarketers. The best one I've seen is when they ring up and pretend to be calling from your bank saying that they're just checking your card details. They already have your details in front of them! Yes they stole them.

They ask you if you're Mr. _____. You answer yes.

Then they quote your account number to you.

Is this your account? Are all these details correct? Yes.

It all sounds very official.

You are then asked to turn your card over, and quote that little 3-digit security number, and you do!

Sir, everything seems to be in order and thank you very much.

That is the only number they did not have! Now they can make as many transactions online as they like using your card.

Use a shredder

Shred all old bank and credit statements, as well as pre-approved credit-card offers, before throwing them into the bin. Use a crosscut shredder as it cuts up paper in two directions: vertically and horizontally. This provides you more security because the shredded paper is in tiny pieces instead of strips which make reconstruction of the documents a lot more difficult.

Secure your mail

Thieves can grab information, simply by stealing it out of your mailbox. Use a locking mailbox to prevent theft or consider getting a P.O.Box. Obviously, if going away on holidays get the post office to hold your mail or ask a friend to clear your mailbox daily.

Online safety

First and foremost, you **MUST** have a comprehensive security package installed on your computer. If antivirus is the only form of protection that you've got, then you're a dead duck! You need a "Triple Shield security package" for complete protection.

Passwords

Preferably, don't use common information like your mother's maiden name, birth date, your SSN or your phone number, or a series of consecutive numbers or keyboard strokes.

If you use online banking or financial services never select a password that matches your username.

Avoid using words that are in the dictionary. Hackers simply carry out a "dictionary-attack" where they rapidly scan through common words, nor should you use the same password over and over. Never give your password to anyone and be sure to change passwords frequently.

If your store passwords locally on your machine be sure the software uses some type of strong encryption.

Phishing and Spoofing

Phishing isn't really new -- it's a type of scam that has been around for years and in fact predates computers. Scam artists did it over the phone for years and called it social engineering. What is new is its modern day delivery vehicle -- spam and faked Web pages.

"Spoofing" attempts to make surfers believe that they are receiving e-mail from a trusted source, or that they are securely connected to a trusted web site, when that's not the case. Spoofing is generally used as a means to convince people to give out personal or financial information by deception.

In "E-mail spoofing", the header of an e-mail appears to have originated from someone or somewhere other than the actual source. Spammers and criminals often use spoofing in an attempt to get recipients to open and possibly even respond to their emails.

"Page Spoofing" involves altering the return address in a web page so that it goes to the hacker's site rather than the legitimate site. This is accomplished by adding the hacker's address before the actual address in any e-mail, or page that has a request going back to the original site, often with a form that looks identical to the legitimate site.

A page spoof might look something like this:

<http://www.paypal.com@thespiesdomain.com/index.html>. The actual domain address is AFTER the @ sign. If you were to surf to this web address and submit any information via a form it would go to the spy and not to PayPal.

Many of these schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick people into divulging financial information such as credit card numbers, account usernames, passwords and social security numbers. By hijacking the brand name banks, e-retailers and credit card companies, such as Citibank, eBay, PayPal, AOL, MSN, Yahoo and EarthLink and Best Buy, phishers often convince people to respond because they look like the "real deal".

Others plant spyware onto PCs to steal credentials directly, often using Trojans and keyloggers. Pharming crimeware directs users to fraudulent sites or proxy servers. The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically.

While online banking and e-commerce is generally very safe, be careful of giving out your personal financial information over the Internet. Banks don't ask for your secret details via email.

Check out these useful links:

<http://www.idtheftcenter.org/index.shtml>

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

The information contained here is published by
www.internethelpsite.com

Copyright © 2005-2007 Joe Jutrisa - *All Rights Reserved*

This is a free report.

Please feel free to pass it on, or refer your friends to the above site for more free information.

If you found these tips helpful and you would like to know more about protecting yourself, your family and your business, just click below to get your own copy of the book, "Internet Security Secrets". It's jam-packed full of information, tips and secrets and is available now at a special introductory price.

www.internetsecuritysecrets.com

