

What to Do if You're a Victim of Identity Theft

If you know or suspect that someone has misused your personal information, report the incident to the three main credit bureaus, and ask them to “flag” your file as belonging to a fraud victim.

Equifax	http://www.equifax.com	1-800-525-6285
Experian	http://www.experian.com	1-888-397-3742
TransUnion	http://www.transunion.com	1-800-680-7289

In addition you should also:

- File a police report.
- Keep detailed records of all the phone calls, interactions, and conversations that you have relating to the theft.
- Notify your credit card issuer if your card has been stolen, and check your statements carefully for new charges.
- Notify your bank if your ATM card has been stolen.
- Request copies of your credit reports to check for newly opened accounts.
- Call the Federal Trade Commission’s Hotline: 1-877-ID-THEFT (1-877-438-4338).

You can, and should, request copies of your credit reports each year to check for suspicious activity: <http://www.annualcreditreport.com>. You can get one free report a year from each of the three bureaus. Space the requests over the course of the year.

Additional Resources

- <http://www.idtheftcenter.org>
- <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm>
- <http://101-identitytheft.com>
- http://www.consumeraffairs.com/news04/2005/ny_id_theft.html
- <http://www.youreviltwin.net/>

If you have any questions about identity theft, please feel free to contact ITS Technology Security Services at security@nyu.edu.



A publication of...

NEW YORK UNIVERSITY
Information Technology Services

© 2006 - NYU. All Rights Reserved. 3-06. ITS Pub.# 2006-10.
<http://www.nyu.edu/its/>. Comments? Write to its.pubs@nyu.edu.

IDENTITY THEFT

NYU Security Awareness Month 2006



More and more of your personal information is stored in an electronic format these days, which greatly increases the risk of that information being accessed by someone without your permission. That person can then illegally use your information (such as your Social Security Number) to obtain money or credit—a practice known as “identity theft.”

Credit card fraud is one of the most common types of fraud committed. Examples of credit card fraud include someone using your name to open a new credit card account, or using your credit card number to purchase items. The next most frequently committed type of fraud is utilities fraud, where someone opens up an account in your name with a gas or electric company. And after utilities fraud comes bank fraud, an example of which would be someone putting up a phishing¹ website that looks as if it belongs to your bank, and then sending you an email message asking that you go to the website to confirm your banking information. The information you entered into the website would then be captured and used to access your bank accounts.

Don't Be a Victim!

There are many ways in which people fall victim to identity theft. We'll go over the non-technical ways first, and then discuss the technical ways. One very common non-technical way of getting personal information about a person is called “dumpster diving.” This is where people search through your garbage looking for any non-shredded personal documents or

Contents

Introduction	1
Don't Be a Victim.	1
Protect Your Digital Data.	2
How Identity Thieves Use Your Info	3
What to Do if You are a Victim of Identity Theft	4
Additional Resources	4

¹ Phishing is a type of email attack in which a criminal claims to be representing a legitimate company or organization in an attempt to trick the recipient into providing their private information, with the purpose of using it for fraud and identity theft.

papers. In this day and age, it is important to own a shredder and to shred any documents containing bank, credit card, loan, or any other financial information before throwing them away.

You are also vulnerable to identity theft if you lose or throw out receipts for your purchases without shredding them. You should take a close look at your receipts when you purchase items with a credit card. Check that only the last four digits of your credit card number are there, rather than the whole number. If you lose a receipt with your whole credit card number on it, you run the risk of some nefarious person finding it and using the number to make purchases.

Another way identity thieves can get information about you is by stealing your wallet. Do you keep credit cards in your wallet? How about your social security card? This is enough information for someone to begin to steal your identity. You may want to avoid carrying your social security card unless you know you're going to need it.

Your identity can also be stolen through a method that is commonly known as social engineering. This is when someone tries to get you to trust them enough to provide some type of personal information. Always be suspicious of any offer that sounds too good to be true, and anyone who asks for your credit card or other personal information over the phone or by email.

Protect Your Digital Data

Now for some of the technical ways someone could steal your identity. How many of you have upgraded to a new computer? What did you do with the old one? Did you throw it out? Before you threw it out, did you remember to erase the hard drive? Did you erase it with a specially made erasing program that prevents others from being able to restore the information? If not, an identity thief could access your old computer and gain access to whatever information you had stored on it. For information on preparing a computer for disposal, see <http://www.nyu.edu/its/security/disposal.html>. Please note that this process is mandatory for any NYU computer you wish to throw out or recycle, but you should also follow those instructions before disposing of a home computer.

The same thing is true about removable media such as zip and floppy disks, CDs, and DVDs. If you don't erase or destroy them before you throw them out, or if you lose them, you are at risk of someone finding them and misusing the information that is on them. Identity theft could also happen if you keep personal or sensitive information on a laptop computer, smartphone or PDA and then you lose that device. Do a Google search on "lost laptop" + "personal information" and you'll get a sense of how frequently identity theft happens in this way.

Another opportunity for identity theft can be created when one company has another company handle their backup tape storage. For example, in 2006, a well-known

company lost backup tapes that held thousands of customers' information for another company. That other company was then forced to tell their customers about this breach, so that they could keep an eye on their credit reports for suspicious charges—a complete nightmare for everyone involved. Again, search Google for "Lost backup tapes" and you'll be shocked to see how often this happens.

Your information could also be stolen if you do business with a company or organization, and that organization or company keeps an electronic file on you. If the computer where your information is kept gets broken into, the intruder can get to your information and then use it without your permission.

Now that so many people are using one or more computers at home, residential wireless networks are becoming widespread. If you use wireless at home, you have to make sure that you are the only one who can access your network, otherwise a stranger can connect to it and have access to all of your information. You can find instructions on how to lock down your wireless network at: http://www.practicallynetworked.com/support/wireless_secure.htm and <http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm>.

Finally, public computers at unsecured cyber-café's are a popular place for identity thieves to get people's personal information. You don't know how much of the information you access stays on that computer after you finish using it, so you should never access your sensitive information from this type of location.

How Identity Thieves Use Your Information

So, once these people actually have your information, just what do they do with it? Well, there are many possibilities: They may call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account and, because your bills are being sent to a different address, they're likely to get away with it for a while before you realize there's a problem. They may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report. They may establish phone or wireless service in your name. They may open a bank account in your name and write bad checks on that account. They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account. They may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction. They may buy a car by taking out an auto loan in your name. They may get identification such as a driver's license issued with their picture, in your name. They may get a job or file fraudulent tax returns in your name. Or, to add insult to injury, they might give your name to the police during an arrest, and if they don't show up for their court date, a warrant for arrest will be issued in your name!