

Identity Theft

No One is Immune!

By Tracey Losco
tracey.losco@nyu.edu

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.

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 papers. In this day and age, it is important to own a

Did You Know?

In New York State, there were more than 7,000 identity theft victims in 2001. New York City had more identity theft than any other U.S. city, with more than 3,300 cases reported—more than twice as many as Chicago, which had the second highest number of cases in the country with 1,470.²

shredder and to shred any documents containing bank, credit card, loan, or any other financial information before throwing them away. As a case in point, a friend's mother, who lives in Philadelphia, sees people driving around her neighborhood every garbage day, stealing garbage bags in the hope that they'll find some type

of information that will help them access someone else's money or personal information. This was so widespread in her area that the city produced a public service announcement, asking people to make sure that they shredded their personal information before throwing it out.

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 your 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

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. See www.nyu.edu/its/pubs/connect/fall04/losco_phishing.html for more information.

2. http://schumer.senate.gov/SchumerWebsite/pressroom/press_releases/PR01342.html

you to trust them enough to provide some type of personal information. This actually happened to me once. I received a phone call from someone claiming to be from the Police Benevolent Association. This individual asked for donations for the PBA, and in return, he claimed that we would receive a courtesy badge. I don't know if any of you have relatives on the police force, but I do, and my own relatives couldn't get me a courtesy badge. Never mind the PBA giving them out to people who make a small donation—I don't think so! What this individual was trying to do was to get me to give him my credit card number, which he then would have used to purchase things, thereby stealing my identity. Always be suspicious of any offer that sounds too good to be true, and anyone who asks for your credit card number or other personal information over the phone or by email.

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 use your old computer to gain access to whatever information you had stored on it. For information on how to prepare your computer for disposal, see 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 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 sen-

sitive information on a laptop computer, smartphone, or PDA and then you lose that device. Do a Google search on "lost laptop" plus "personal information" and you'll get a sense of how frequently identity theft happens in this way.

Did You Know?

You can, and should, request copies of your credit reports each year to check for suspicious activity: www.annualcreditreport.com. You can get one free report a year from each of the three bureaus linked to on this site, so you should space the requests over the course of the year.

Another opportunity for identity theft can be created when one company has another company handle their backup tape storage. For example, this year, 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 www.practicallynetworked.com/support/wireless_secure.htm and <http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm>.

Finally, public computers at unsecured cyber-café 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!

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
www.equifax.com, 800-525-6285
- Experian
www.experian.com, 888-397-3742
- TransUnion
www.transunion.com, 800-680-7289

In addition you should:

- File a police report
- Keep detailed records of all the phone calls, interactions, and conversations 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 (see "Did You Know" on p. 19 for instructions).
- Call the Federal Trade Commission's Hotline: 1-877-ID-THEFT (1-877-438-4338)

ADDITIONAL RESOURCES

- www.idtheftcenter.org
- <http://101-identitytheft.com>
- www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm
- www.newyork.bbb.org/identitytheft
- www.oag.state.ny.us/consumer/tips/identity_theft.html
- www.consumeraffairs.com/news04/2005/ny_id_theft.html
- www.youreviltwin.net

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

Tracey Losco is a Network Security Analyst in ITS' Technology Security Services.

<< Continued from "The TeraGrid," p. 5

(a TeraGrid member site), envisions important research opportunities for her group in the use of TeraGrid facilities at NYU, should they become available.

Her group would like to use these resources to further their research already underway at the NCSA. This research involves the mapping out of the complete chemical reaction pathway for DNA polymerase beta repair, in order to better under-

stand the enzyme's fidelity mechanism, and the simulation of the folding dynamics of chromatin fiber, in order to investigate transcription regulation processes.

To qualify for participation in the TeraGrid project, NYU would need to share its computing resources with other TeraGrid participants, and in exchange, NYU researchers would gain access to a variety of resources outside the University. ITS, in col-

laboration with NYU researchers, is actively exploring the potential benefits of entering into such an exchange. Stay tuned to future issues of *Connect* for more information about this project and supercomputing at NYU.

Randy Wright is a Senior Systems Administrator in ITS' .edu Services' eServices division.

<< Continued from "Next Generation Internet Technology," p. 11

not officially support IPv6, although an experimental Microsoft implementation can be enabled manually. Its capabilities are also limited, and to date, Microsoft operating systems cannot make use of IPv6 for DNS operations.¹²

As we continue to deploy IPv6 connectivity on campus in support of academic and research activities and new services, we will also endeavor to collaborate with other organi-

zations involved in this endeavor. Recently, the United States Government Accountability Office met with NYU to learn about our experiences with IPv6 in order to aid them in writing their report to Congress on IPv6 technology. Through such relationships, we hope to not only foster IPv6 technology globally, but also further it as an enabler of research and education.

For additional information about

IPv6 technology, see www.ipv6.org. If you are interested in discussing the possibility of using IPv6 in support of your research or academic endeavors, please contact the ITS Faculty Technology Services Center at its.ftc@nyu.edu or 212-998-3044.

Jimmy Kyriannis is Senior Technology Architect for NYU Information Technology Services' Communication & Computing Services.

12. The Domain Name System is a worldwide database that translates Internet Domain Names into their IP addresses (e.g., www.nyu.edu translates into 128.122.108.74).