GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Loosing Yourself:
Identity Theft in the Digital Age

By Greg Surber

For most of us, giving out personal information like our home telephone number or driver's license number is an everyday occurrence. Something we do with every check we write or online order we place. But do we really know what happens to that information once it leaves our hands? More than ever, the information explosion, aided by an era of easy credit, has led to the expansion of a crime that feeds on the inability of consumers to control who has access to sensitive information and how it is safeguarded. That crime is identity theft.

What is Identity Theft, anyway?

"*Identity theft and identity fraud…refer to all types of crime in which someone wrongfully obtains and uses another person's personal data…*"
US Department of Justice, Criminal Division, Fraud Section report.

Identity theft is when someone takes your personal information—like your name, address, social security number, mother's maiden name—and uses it to establish unauthorized credit and charge items in your name. And finding someone's personal information has never been easier. Web sites like Any Who (http://www.anywho.com) and US Search (http://www.1800ussearch.com)have made finding personal information just a click away. With this increase in easy access to personal information, reports of identity theft have risen dramatically over the past few years. According to the Trans Union credit-reporting Agency, the number of calls or complaints has jumped from 35,000 in 1992 to over 550,000 in 1998. That's an increase of more than 1500% in only six years. And that number is expected to nearly double to about 980,000 by the end of 2001. Meanwhile, a survey of identity theft victims by the California Public Interest Research Group (CALPIRG) and the Privacy Rights Clearinghouse found that the average total fraudulent charges made on each account was $18,000. That average includes totals ranging from $250 to more than $200,000 per account.

What is being done to protect my personal information?

In 1998, the United States Congress enacted US Code : Title 18, Section 1028, more commonly known as "The Identity Theft and Assumption Deterrence Act." Section 1028 legally defines both identity theft (knowingly possessing an identification document other than one issued lawfully for the use of the possessor) and identity fraud (knowingly possessing a false identification document) and sets punishments for both including both fines and possible

© SANS Institute 2000 - 2005 Author retains full rights.

prison terms. This law was intended to protect the American people from this newly emerging threat. It has gone a long way by defining the crime and in pronouncing appropriate punishments for its infraction. Unfortunately, the problem doesn't lie within the law, it lies within assumptions.

Federal law limits a consumer's financial liability for credit card fraud to $50 per account. Therefore, it is the assumption that the credit issuing company, not the consumer, is the main victim. The credit issuing company, after all, is left with the bulk of any financial loss incurred from the illegal use of these stolen accounts. However, the stories of victims of identity theft facing the ruin of their once perfect credit rating can be staggering. In the central district of California, for example, a woman pleaded guilty to federal charges of using a stolen Social Security number to obtain thousands of dollars in credit and then filing bankruptcy in the name of her victim. Another victim, also from California, relates the story of how someone received a duplicate California Driver's License from the DMV with the victim's information. With this stolen identity, the thief rented properties, signed a one-year lease for one residence, bought a brand new truck, and had liposuction performed via a line of credit. The worst part was the federal prison of Chicago booked the thief under the victim's name when the thief was caught smuggling 3,000 pounds of marijuana.

Another underlying assumption is one of guilt over innocence. The standard "burden of proof" process, which our system of law is based upon, has been seemingly reversed in cases involving identity theft. Whereas other criminal cases force prosecutors to show, beyond a reasonable doubt, that the defendant committed the crime in question, identity theft cases force the victim to prove their innocence by proving their identity. Once that battle is won, they still must somehow clear their names of all the bad-credit ties.

What can I do to protect myself?

The first thing you must do is protect your personal information. There are companies, such as ZeroKnowledge (http://www.zeroknowledge.com), who have developed privacy solutions that can help preserve your personal information, and protect you from web pages and applications that attempt to remove your personal information from your computer without your consent. It's amazing how much can be learned about a person from something as seemingly mundane as a phone number. Online people-finder services (such as http://www.AnyWho.com or http://www.1800USSearch.com) are making it increasingly easy for a would-be thief to take your phone number, enter it online and discover your full legal name, as well as your current and past addresses. Once an identity thief has your name and address, they can go to one of the so-called "online detective" sites, pay a small fee and get a lot more information about you. Some sites even offer to find Social Security Numbers based solely on name and address.

© SANS Institute 2000 - 2005 Author retains full rights.

The average Internet users' primary asset is their personal information, and this asset should be closely guarded. Whenever you are surfing the web, installing shareware or gossiping on IRC, always be skeptical. By creating online profiles and storing your personal information on your computer you eliminate one of the original security features of the Internet, anonymity.

For the more wary of us, many insurance companies have begun offering Identity Insurance. Travelers insurance Group, for example, offers Identity Theft insurance as both an add-on to your existing home-owner's insurance account or as its own stand-alone Identity Theft insurance account. The Traveler's Insurance Group homepage describes their services on their web page (http://www.travelerspc.com/personal/theft/affordable.cfm :

> For just an additional $25 annual premium, you can have Identity Fraud Expense Coverage added to your Travelers homeowners, condo or renters policy with a coverage amount of $15,000 and a $100 deductible…
>
> Should you prefer to buy identity theft protection under a free-standing policy, Travelers has the Personal Financial Protection Policy. …depending on the dollar amount of protection that you choose, the Personal Financial Protection Policy's protection can be obtained for you and your family for a premium that works out to less than $5 per month.

While it may not be possible to completely protect yourself from identity theft, there are a few basic things you can do to minimize the risk (from a report by the Federal Trade Commission):

- Before you reveal any personally identifying information, find out how it will be used and whether it will be shared with others. Ask if you have a choice about the use of your information: can you choose to have it kept confidential?
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address to cover his tracks.
- Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after it has been delivered. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up.
- Put passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

© SANS Institute 2000 - 2005 Author retains full rights.

- Minimize the identification information and the number of cards you carry to what you'll actually need.
- Do not give out personal information on the phone, through the mail or over the Internet unless you have initiated the contact or know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers and even government agencies to get you to reveal your SSN, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with whom you do business have the information they need and will not ask you for it.
- Keep items with personal information in a safe place. To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, bank checks and statements that you are discarding, expired charge cards and credit offers you get in the mail.
- Be cautious about where you leave personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.
- Find out who has access to your personal information at work and verify that the records are kept in a secure location.
- Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible.
- Don't carry your SSN card; leave it in a secure place. Order a copy of your credit report from each of the three major credit reporting agencies every year. Make sure it is accurate and includes only those activities you've authorized. The law allows credit bureaus to charge you up to $8.50 for a copy of your credit report. Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills and whether you've been sued, arrested or filed for bankruptcy. Checking your report on a regular basis can help you catch mistakes and fraud before they wreak havoc on your personal finances.

What can an identity thief really do with my information?

Starting with just one piece of information about you, be that your full name, address or phone number, an identity thief can find all three. Online people finding web sites, like WhitePages.com (http://www.whitepages.com), offer free searches based on name, address or phone number. Now that the thief has these three pieces he need only visit 77 Investigations (http://www.77investigators.com), pay their $45.00 fee and obtain your Social Security Number. Or, for just $55.00 more they will provide them with all of this additional information:

- Real Estate owned by the subject (Asset)

© SANS Institute 2000 - 2005 Author retains full rights.

- Tax Assessor Information (Asset)
- Property Characteristics (Asset)
- Neighbor Names, Phone Number, Date Of Birth
  (Information varies from neighbor to neighbor)
  Very valuable for personal references and finding friends, lovers or allies.
- AKA'S (Other names known to be used by the subject) (Credibility)
- Corporate Records (Asset)
- Subject Birth Month & Year: Day included when available.
- Dates subject was reported at former addresses (Credibility)
- Listed Phone Numbers
- DEA Registrants
- Marriage Records
- Divorce Records
- Search to find death records associated with the subject's social security number. (Using a social security number of a deceased person)
- Other persons using the same social security number as the subject (Possible identity fraud)
- Ucc Records (Asset)
- Possible relatives with current address, phone number, and date of birth. (Information varies from relative to relative)
- Documented Vessels Owned (Asset)
- Watercraft Owned (Asset)
- Aircraft Owned (Asset)
- Licensed Pilot Information Check
  (Possible employment, flight risk or link to other assets)

Obtaining a credit rating for someone with this much information about them (actually, all that is needed is name, address and Social Security Number) is very easy. An identity thief need only contact one of the main credit reporting agencies (Trans Union (1-800-680-7289), Experian (TRW) (1-800-397-3742), or Equifax (1-800-685-1111)) and explain that they are trying to rent a house. The agency will, for a small fee, set up a credit report terminal which the thief can then use to get a full credit report. That credit report allows the identity thief to scope out the most promising subject(s) based on credit rating and available credit.

Finally, a little social engineering is all that is needed to complete the theft. Using their legally gotten information, the identity thief can call the phone company and ask for the phone bill of his intended victim to be forwarded to a new address for a short time. After verifying their customer's identity, the phone company is more than happy to oblige and soon the thief has a listing of friends and family members complete with phone numbers. By asking the right questions, the thief is able to uncover even more personal information about his target.

© SANS Institute 2000 - 2005 Author retains full rights.

Help! My identity has been stolen. What do I do now?

In his new book “Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Destruction”, author and information security expert Winn Schwartau details a very personal experience with identity theft. His cousin, Bill Waters, a 66 year old Korean War veteran first discovered that someone had stolen his identity when several credit issuing companies began sending him letters demanding payment for goods or services he had not ordered. Within a six month period his total debt leapt to over $250,000 and, despite all of their efforts to explain to the credit companies that the debt was not theirs, the lawsuits soon began. Even his own bank, which he had been with for years, had issued a line of credit against his home to the identity thieves. Less than two months later, Bill Waters died of a massive stroke and heart attack.

If you find that you have been the victim of identity theft, all is not lost. There are still a few things you can do.

- First, call the police and file a report. Make sure to get a copy of that report, as you’ll need it in dealing with banks, credit card companies and credit bureaus.

- Second, call the fraud departments of all three major credit bureaus: Equifax (1-800-525-6285), Experian (1-888-397-3742) and Trans Union (1-800-680-7289). Make sure to ask that your account be flagged with a fraud or security alert.

- Third, if your Driver’s License number has been compromised, you should contact your local Department of Motor Vehicles. They will need a copy of your police report to change the number.

- Finally, if your Social Security number has been used, you can request a new one from your local Social Security Administration office.

The biggest problem with cases involving identity theft is that the standard "burden of proof" process inherent in our legal system works against the victim. In typical cases, the state must establish, beyond a reasonable doubt, that the defendant is guilty. However, in identity theft cases, the victims are forced to try to prove their innocence. The trouble is, even after identity theft victims successfully prove they're not the ones running up huge credit card bills, it may take years to clear their names from various bad-credit reports.

© SANS Institute 2000 - 2005 Author retains full rights.

What can be done to reform the system and make it work for the victims instead of against them?

Article 12 of the Universal Declaration of Human Rights says,

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

On December 10, 1948, the United States Government, along with many other nations of the world, signed it. Yet, here we are, more than 50 years later, in a world where anyone with $100 and a computer can learn enough about you to steal who you are, run up huge debt and leave you to clean up the mess.

Privacyrights.org (http://www.privacyrights.org/ar/idtheft2000.htm) has developed a possible list of recommendations to help law enforcement and victims of identity theft work together better when the time comes:

1. Give law enforcement the resources and education to adequately investigate the crime. They should respect victims, write police reports, and take steps to pursue and arrest the perpetrator. The results from the survey show that when law enforcement did actually take steps to investigate the perpetrator, they were often successful. In many cases, a victim will not feel that his or her case is completely solved until the thief is behind bars and cannot commit the crime again.

2. Make identity theft a crime against the true victim in states where it is not. In states where identity theft is a crime, criminals should face more severe punishment, and victims should have the right to sue those partly at fault for their stolen identity -- the creditors and credit bureaus. A few of the victims surveyed reported that their thieves had served short prison terms, between two months and three years, or that they were held on probation.

3. There needs to be a clearinghouse of information where victims can turn for advice. Establish an agency or office whose job it is to make phone calls on behalf of the victim to the credit bureaus, creditors, and collection agencies. This would help relieve the hundreds of hours that victims reported spending on their identity theft cases.

© SANS Institute 2000 - 2005 Author retains full rights.

4. Make it harder for creditors to grant credit to an identity thief by creating fraud alerts that work and by requiring creditors to be more vigilant in their investigation into the person seeking credit. Most of the cases reported could have been prevented if the first creditor receiving the fraudulent application had looked more closely at the information on the application, or had attempted to contact the original person on file to check if the applicant was the same.

5. Creditors and credit bureaus should assist victims in both investigating the crime and repairing their damaged credit. Victims should be able to obtain the original application that was fraudulently completed by the thief with the victim's information. Many victims reported that they had been refused copies of the fraudulent application. They said it would have been easier to apprehend the perpetrator if this information had been available.

6. There should be laws prohibiting the sale of personal information and the release of a credit report without prior authorization and a password known only by the victim. The fact that almost half of the victims' fraud recurred on their credit report demonstrates that the current system of fraud alerts is not working.

Until such time as Congress sees identity theft for the problem it is and creates laws to better protect our valuable personal information, our best defense is vigilance.

- Check your credit reports at least once a year.
- Avoid using your Social Security Number as an identifier, instead make up a nine-digit number and use that.
- Carefully check all credit card bills and report any unauthorized activity immediately.
- Shred all sensitive documents before throwing them out.
- See if your credit card companies offer cards with photos on them. If they do, get one.

Most people don't think twice about giving out their personal information. They write their phone number on the check they hand the waiter, they type their home telephone number into the box on their computer screen. But are they giving away too much? Some people have lost their good credit rating to the predators who wander the dark alleys of the Internet, some have lost much more.

© SANS Institute 2000 - 2005 Author retains full rights.

References

Benner, Janine, Beth Givens and Ed Mierzwinski. " Nowhere to Turn: Victims Speak Out on Identity Theft." PrivacyRights.org. May 2000. URL: http://privacyrights.org/ar/idtheft2000.htm

Federal Trade Commission. "ID Theft: When Bad Things Happen to Your Good Name." February 2001. URL: http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Fraud Section, Criminal Division, U.S. Department of Justice. "Identity Theft and Fraud." 05 June, 2000. URL: http://www.usdoj.gov/criminal/fraud/idtheft.html

Kabay, M.E. "Identity Crisis." Information Security Magazine. July 2000. URL: http://www.infosecuritymag.com/articles/july00/columns3_logoff.shtml

Madine, David. "Prepared Statement of the Federal Trade Commission on 'Identity Theft'." Federal Trade Commision. 20 May, 1998. URL: http://www.ftc.gov/os/1998/9805/identhef.htm

Schwartau, Winn. Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Destruction. New York City: Thunder's Mouth Press, 2000.

Travelers Insurance Center. 2001. URL: http://www.travelerspc.com/personal/theft/affordable.cfm

Additional Web Sites Referenced

1-800 Search (http://www.1800search.com)

AnyWho (http://www.anywho.com)

Zero Knowledge (http://www.zeroknowledge.com)

White Pages (http://www.whitepages.com)

77 Investigations (http://www.77investigations.com)

© SANS Institute 2000 - 2005 Author retains full rights.