Global Information Assurance Certification Paper

Identity Theft: Imitation Isn't the Sincerest Form of Flattery

Reg Washington
January 31, 2005

GIAC Security Essentials Certification (GSEC)
Practical Assignment v1.4c option 1

Abstract

Identity Theft is the nation's fastest growing crime according to FBI statistics and identity theft/fraud is the fastest-growing category of Federal Trade Commission (FTC) complaints. An estimated 27.3 million Americans have been victims of some form of identity theft within the past five years according to a September 2003 FTC survey including almost 10 million people in 2002 alone. According to the survey, last year's identity theft losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion out-of-pocket expenses (1).

The purpose of this paper is to completely define the threat of identity theft. The paper will outline the following: how identity theft occurs, tips to avoid becoming a victim, and ways to recognize if you've been victimized. I will also explore the role of technology in aiding and combating identity theft and how identity thieves use your personal information. Additionally, this paper will provide details on steps to take if you become a victim. Finally, I will discuss some of the identity theft legislation that has been enacted or being proposed.

Introduction

Unfortunately, the crime of identity theft is not only one that I have chosen to research but one that I was also a victim. In 2003, my credit card information was used to purchase $1000 worth of stereo equipment at an electronics store in Denver, Colorado. The credit card was a debit/check card issued by my local bank. So when purchases were made using the card, the money would be automatically withdrawn from my checking account. As a result, I started receiving overdraft notices for checks which had insufficient funds. Needless to say this was quite a surprise to me. This caused me to investigate the reason for the overdraft charges. I reviewed my checkbook register and noticed my balance was significantly higher than what the bank records showed. I notified the bank to ask them about recent transactions and noticed a $1000 debit/check card charge for electronics equipment at a store in Denver, Colorado.

The process of clearing up the discrepancy took approximately 3 to 4 months. Not only did I have to be reimbursed for the charge and receive a new debit/check card but I was also credited for overdraft charges which I had been charged. And in conjunction with my bank, I had to work with the store to prove the charges were not done by me. Needless to say, my experience with identity theft was one I will not soon forget.

As a result of this experience and being an information security professional, I am much more aware of protecting my personal information in my everyday life. I believe most people would be surprised how much there personal information is at risk for being exploited on a daily basis.

What is Identity Theft?

Identity Theft is defined as the use of a person's personal information by another to commit fraud or other crimes. The most common form of identity theft occurs when someone illegally obtains another person's social security number, driver's license number, date of birth, or any other pertinent personal information and uses it to open fraudulent accounts, obtain false loans, or somehow benefit financially from it (2).

The types of identity theft are broken down into the following:

- Financial fraud – type of identity theft that includes bank fraud, credit card fraud, computer and telecommunications fraud, social program fraud, tax refund fraud, mail fraud, and many more. A total of 25 types of financial identity fraud are investigated by the United Secret Service.
- Criminal activities – type of identity fraud involves taking someone else's identity in order to commit a crime, enter a country, get special permits, hide one's own identity, or commit acts of terrorism. The criminal activities can include:
  - Computer and cyber crimes
  - Organized crime
  - Drug trafficking
  - Alien smuggling
  - Money laundering (3)

How Identity Theft Occurs

Identity Theft is very different from what might be considered a "traditional" crime. Usually there is no one doing physical harm to you or holding a weapon and demanding information. The object is to be stealth and go undetected in order to use someone else's personal information for as long as possible. Skilled identity thieves use a variety of methods to gain access to your personal information. For example,

- Hacking into a businesses' computers
- Dumpster diving – rummaging through trash in an attempt to find personal information
- Steal personal records from their place of employment
- Skimming – using a special information storage device to steal debit/credit card numbers as the card is being processed
- Steal wallets and purses containing identification and credit cards
- Steal mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.
- Complete a change of address form to divert your mail to another location

so they can receive your mail containing personal information
- Steal personal information from your home (4)

In addition to the methods listed above, some other social engineering methods of identity theft are pretexting, phishing, shoulder surfing, bribing, and eavesdropping. Pretexting is the illegal practice of obtaining personal information under false pretenses by pretending to be someone else. For example, if someone calls your bank or credit card company and pretends to be you. Phishing scams are online crimes that use "spam" email to direct internet users to websites controlled by hackers that look like legitimate e-commerce websites. Users are asked to provide sensitive, personal information which is then captured by the hackers. Shoulder surfing is a form of social engineering which occurs when someone watches as you type in your personal information. Bribing is offering money or other incentives to someone in order to obtain someone else's personal information. Eavesdropping is listening or overhearing someone's private conversation in order to hear confidential information.

Although identify theft can occur in many ways as detailed above – some being highly-technical and sophisticated, theft of wallets and dumpster diving are the most common ways identity theft occurs. So despite the advancements in technology, more simple means are used to steal your personal information.

Reasons for Identity Theft

According to Cath Everett, the reason for the alarming increase in identity theft is easy to understand: there's far more personal data around to steal (5). Not only is there more personal data to steal there is more technology available to both handle the storage and security of the data. Ironically, the same technological advancements make it easier for hackers to steal data.

For example, despite concerns about security and privacy, the use of e-commerce has grown steadily each year. This growth indicates that more people have access to internet technology. This means more personal information is available for identity thieves.

Is Identity Theft a Big Deal?

Yes, and let me explain further. The crime of identity theft has definitely gotten plenty of attention over the past few years. If you are fortunate enough not to be a victim of identity theft directly, you still might be a victim indirectly. The cost of identity theft is often absorbed by businesses that ultimately have to pay for unauthorized charges made by identity thieves. However, businesses don't just absorb these costs without passing them on to the consumer in the form of higher fees or penalties. So indirectly you're a victim because you ultimately pay the price.

You can control some personal risk but you can't control or often even find out

about the risk companies you do business might potentially expose your personal information. Companies that store highly sensitive and personal information often put that information at risk. For example, the theft of a laptop belonging to a Wells Fargo Bank consultant posed a risk to the personal information of thousands of bank account holders (6). Another incident occurred when a sale of surplus computers owned by the State of Virginia exposed employee evaluations, credit card numbers, and other sensitive data of Virginia citizens, because the hard drives hadn't been wiped clean before going to auction (7).

Identity theft can also cause nonmonetary harm to the lives of individuals. Even if financial institutions don't hold victims liable for fraudulent debts, victims might still feel the emotional harm of feeling an "invasion of privacy" knowing that someone used their personal information, and "trauma" from the significant amount of time spent trying to resolve the problems caused by identity theft. The tangible types of nonmonetary harm that can be experienced range from being denied credit or other financial services, or actually being subjected to criminal investigation, arrest, or conviction.

Steps to Take if you've Been Victimized

Even if you are very careful about your personal and financial information you still can become a victim. But if you are diligent about checking your banking accounts, monthly bills, and review your credit report periodically, you will detect identity theft early. Early detection makes the process of correcting accounts and credit problems much easier. The following steps should be taken immediately if you discover that your identity has been stolen:

- Place a fraud alert on your credit report. This is an important step in regaining your good name and good credit.
- Close compromised accounts. If you've been victimized, close those accounts immediately.
- Call your credit card company. If you review your monthly statement and find an item you wish to dispute, call the credit card company immediately.
- Contact your bank. Call your bank if you discover checking or savings account discrepancies.
- File a complaint with the Federal Trade Commission.
- File a report with your local police or the police where the identity theft took place.
- Contact the local post office if you suspect your mail has been redirected do to an identity thief submitting a change of address form.
- Contact the Social Security Administration if you suspect your Social Security Number has been used fraudulently.
- Document your actions. You should document the time and money you

spend relating to the theft.

The Role of Technology in Identity Theft

In an ever evolving technological age, let's examine the role technology plays in preventing identity theft and tips to safeguarding information stored on your computer.

- Use of antivirus software. Viruses can often cause your computer to send out files or other stored information.
- Use a firewall. A firewall can be used to limit an application's access to your computer. Hackers can take over your computer and access the sensitive information stored on it.
- Encryption of the files you store on your PC. Encryption uses keys to lock and unlock data while it's being transmitted over the Internet, so that only the intended recipient can view the data. Encryption is also used to protect email messages and attachments stored on your PC. You can verify if websites use encryption to transmit your personal information. In Internet Explorer this is done by checking the yellow lock icon on the status bar (8).
- Use of authentication. Authentication is the method used to identify you via username and password when accessing personal information on your PC or online.
- The use of biometrics. Biometrics is a type of authentication that uses individually unique physical attributes such as fingerprinting, iris/retina, facial structure, speech, facial thermograms, hand geometry and written signatures (3).

Minimize your Risk

An important part of preventing identity theft is minimizing the exposure of your personal information. The following tips will help minimize your risk of being a victim of identity theft:

- Many websites have an automatic log-in feature that saves your user name and password. Don't use this feature because it makes it easy for hackers to gain access to your personal information stored on websites.
- Delete all personal information from your computer before you dispose of it.
- Don't store personal information in email files. Emails can be easily read by hackers.
- Make sure you are aware of what websites do with the information that

you provide to them. They should have a documented privacy policy.
- Don't open or respond to online solicitations for personal information.
- Keep track of all your internet transactions and verify your credit card statement for accuracy.
- Check your email for order confirmation after making online purchases.
- If you subscribe to any web-based service, change your password immediately if you receive an email confirmation of your account and/or password.

Organizations Struggle with Identity Theft

So far I've analyzed identity theft from a consumer perspective. But another very important perspective is that of organizations that attempt to prevent identity thieves from penetrating their networks. Since organizations store such a magnitude of data they are a prime source to exploit. Companies are also reluctant to admit being a victim of hackers because of the public embarrassment and loss of potential business.

Companies that are targeted can fall into the following categories: prime targets, secondary targets, and random targets. Prime targets are generally companies that have financial data and have large amounts of personal information that would have huge financial benefit. Although these targets are desirable they also pose a challenge to hackers. These companies tend to have more stringent security controls to deal with potential threats. Secondary targets are smaller companies in comparison to prime targets. These targets are becoming more desirable for hackers because they generally will not have the resources and stringent security controls as do larger companies. Most smaller companies don't have the proper intrusion detection and response capabilities necessary to deal with a breach in security. Often times they will not offer as much identity-rich information as primary targets. Random targets are those that are random in nature as far as targeting. They can be either large or small companies. Hackers depend on social engineering tactics to gain access to these targets. Employees of these companies are a key factor in preventing hackers from gaining access to personal information.

Companies also are faced with additional costs related to identity theft. Those costs are manifested through the necessity for banks, credit card companies, and consumer reporting agencies to add to the staffing of their fraud departments. These departments are used for fraud prevention, detection, investigation, and prosecution.

Identity Theft Legislation

Most federal and state legislation has recognized that identity theft is a serious crime across the nation. So a challenge to lawmakers is to ensure that relevant

legislation is effectively enforced.

Federal legislation has been proposed and/or enacted over the last few years to combat the spread of identity theft. Some of the legislation includes the Fair and Accurate Credit Transactions Act, the Identity Theft Victims Assistance Act, and the Identity Theft Prevention Act.
The Fair and Accurate Credit Transactions Act ensures that citizens have the ability to build good credit and have their credit information protected from identity theft. The identity theft portions of the Act are as follows:

- Consumers have the right to their credit report free of charge every year, in order to review for unauthorized activity.
- Require merchants to leave all but the last five digits of a credit card number off store receipts.
- Create a national system of fraud detection
- Establish a nationwide system of fraud alerts for consumers to place on their credit files.
- Requiring regulators to devise a list of red flag indicators of identity theft, drawn from the patterns and practices of identity thieves.
- Requiring lenders and credit agencies to take action before a victim even knows a crime has occurred (9).

The Identity Theft Victims Assistance Act was proposed to help prevent identity theft and mitigate harm to victims of that crime. It has the following identity theft provisions:

- Establishes a nationwide process for victims of identity theft to obtain business records related to identity theft.
- Clarified that for victims of identity theft, that statute of limitations for the Fair Credit Reporting Act will be five years, rather than the current two years.
- Requires consumer credit reporting agencies to block reporting of bad credit that arises from identity theft.
- Expands the role of the federal Coordinating Committee on False Identification beyond the current mandate to review federal enforcement of identity theft law (10).

The Identity Theft Prevention Act was proposed to provide consumers with access to information that may reveal indications of identity theft or the source of erroneous information resulting from identity theft. It has the following identity theft provisions:

- Increase penalties by two years for anyone who commits “aggravated identity theft” in order to perpetrate a serious federal predicate offense.
- Increase penalties by five years for anyone who commits identity theft for

the purpose of committing a terrorist act.
- Make it easier for prosecutors to prove identity theft by stating that as long as criminal intent is proved no further proof is required.
- Add the word “possesses” to current law so that prosecutors can go after identity thieves who possess false identity documents with the intent to commit a crime.
- Increase maximum term of imprisonment for ordinary identity theft and for possession of false identification documents from three to five years (10).

Conclusion

The increase in identity theft can be attributed to the fact that with progress there are often problems. The fact that more and more people are doing business online and more personal information is out in the public makes it vulnerable for identity thieves to steal. There are several steps that can be taken to protect you from being a victim. Even when steps are taken to protect yourself, there are still identity thieves/hackers looking to exploit any possible weakness and vulnerability in the process. In addition to the precautions that a person can take to combat identity theft, there are laws and agencies setup to deal with victims and perpetrators of the crime.

References

1) Oklahoma University Police Department. “Identity Theft – Part 1 – Introduction to Identity Theft – The Police Notebook” 18 October 2004. URL: http://www.ou.edu/oupd/idtheft.htm

2) Encyclopedia.com URL: http://www.encyclopedia.com/html/i1/identthft.asp

3) Howstuffworks. “How Identity Theft Works” URL: http://computer.howstuffworks.com/identity-theft.htm

4) Federal Trade Commission October 2003. URL: http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.htm

5) Everett, Cath. “Identity Theft: How You can Protect and Survive” Computeractive 18 June 2004. URL: http://www.computeractive.co.uk/features/1156002

6) Kawamoto, Dawn. “Wells Fargo Computers Stolen” ZDNet 3 November 2004 URL: http://news.zdnet.com/2100-1009_22-5437481.html

7) Auditor of Public Accounts Special Review. “Surplus Computer Equipment Data Removal” October 2003 URL: http://www.apa.state.va.us/data/download/reports/audit_local/surplus03.pdf

8) Microsoft. “Phishing Scams: 5 Ways to Help Protect Your Identity” 8 July 2004 URL: http://www.microsoft.com/athome/security/email/phishingdosdonts.mspx

9) The White House. “President Bush Signs the Fair and Accurate Credit Transactions Act of 2003” 4 December 2003 URL: http://www.whitehouse.gov/news/releases/2003/12/print/20031204-3.html

10) Fight Identity Theft. “Identity Theft Legislation” URL: http://www.fightidentitytheft.com/identity-theft-laws.html

Last Updated: October 18th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event