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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Identity Theft Attacks & Countermeasures

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4c Option 1

Brian Nolan
October 21, 2004

© SANS Institute 2005, Author retains full rights.

Abstract

A report by the Federal Trade Commission, published in September of 2003, concluded that 9.91 million Americans were victims of identify theft in 2002, with business losses of 47.6 billion dollars and consumer loses of 5 billion dollars.[1] On July 15th 2004, at the signing of the Identity Theft Penalty Enhancement Act, President Bush said that identify theft is "one of the fastest growing financial crimes in our nation".[2] Attacks against people's personal and confidential information are on the rise and every citizen is at risk. It is essential that individuals take a proactive position in securing their personal information and defending themselves against these serious crimes.

In this paper I will examine various types of attacks used by criminals to steal personal information and I will discuss countermeasures that can be used to defend against these attacks. I will begin by talking about the crime of identity theft and the related laws. Next I'll look at the different types of identity theft and the motivations behind the crimes. By understanding the criminal objectives, it will become easier to recognize the types of personal information that the attackers require, and often target, in order to achieve their goals. I will then explore some specific attacks being used today to compromise confidential information along with the defense strategies that can be used to protect information against these attacks. In conclusion, I will briefly discuss the detection and response process for victims of identity theft.

The Crime of Identity Theft

Identity theft is a crime in which someone wrongfully obtains another person's personal information and then uses that information to commit fraud. The Identity Theft and Assumption Deterrence Act of 1998 defines the crime as a circumstance in which someone "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law or that constitutes a felony under any applicable State or local law"[3] It is this Act that makes identity theft a federal crime which carries a maximum penalty of 15 years in prison plus fines and criminal forfeiture. President Bush recently increased the penalties for identity theft when he signed into law the Identity Theft Penalty Enhancement Act in July, which adds two years to prison sentences for criminals that use stolen credit card numbers and other personal data to commit crimes. Often the crimes of identity theft violate other federal laws including computer fraud, mail fraud, Social Security fraud, credit card fraud,

---

[1] "Federal Trade Commission – Identity Theft Survey Report." September 2003
URL: http://www.ftc.gov/os/2003/09/synovatereport.pdf (October 2004)
[2] "President Bush Signs Identity Theft Penalty Enhancement Act." July 15, 2004.
URL: http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html (October 2004)
[3] "Identity Theft and Assumption Deterrence Act of 1998."
URL: http://www.identitytheft.org/title18.htm (October 2004)

© SANS Institute 2005 Author retains full rights.

financial institution fraud, and wire fraud. Each of these federal laws includes its own set of penalties. Violations of federal law pertaining to identify theft are investigated by law enforcement agencies such as the Federal Bureau of Investigation, the US Secret Service, the Social Security Administration Office of the Inspector General, and the US Postal Inspection Service. In addition, many states have created statutes related to identity theft and impose penalties for violation of these state laws.[4]

Types of Identity Theft

The Identity Theft Resource Center, a non-profit organization which helps people prevent and recover from identity theft, classifies crimes of identity theft into the following four categories: financial ID theft; criminal ID theft; identity cloning; and business or commercial ID theft.[5]

Financial ID theft involves crimes where the objective is financial gain through the wrongful use of someone's personal information. The criminals involved with these types of crimes steal personal data and then use that information to pose as their victim in order to establish new lines of credit and services in the victim's name and/or steal existing savings and credit. Crimes of this type are typically a hit and run type situation where the criminal gains access to accounts in the victim's name, quickly exhausts the funds or credit lines and then disappears, leaving the financial burden on the victim. Often the criminal will have the bills and statements for these accounts sent to an address other than the victim's, in order to keep the victim unaware of the unauthorized withdraws and transactions. In many cases it is not until a collection agency tracks down the victim or until a victim is denied credit that he or she becomes aware of the crime against them.

Criminal ID theft involves fraud with the objective to transfer legal accountability to the victim. The criminals involved with these types of crimes steal personal information and then use that information to assume the identity of their victims during encounters with law enforcement. A criminal that is stopped by law enforcement for a violation of the law may use false documentation, such as a fake driver's license with the victim's name, address, date of birth, and driver's license number, but with the criminal's own picture, in order to pose as the victim. If a citation is issued, it is issued to the victim and not the actual criminal. If it is a more serious crime and the criminal is released from police custody and then fails to show up for court, an arrest warrant is issued for the victim and not the actual criminal. If this happens, the victim may be caught completely unaware when arrested by police. Criminal ID theft is used in crimes ranging from simple traffic tickets to felonies such as burglary and car theft.

[4] For a list of identity theft statues as of July 2003 see:
URL: http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm (October 2004)
[5] URL: http://www.idtheftcenter.org/cresources.shtml (October 2004)

© SANS Institute 2005 Author retains full rights.

Identity cloning involves crimes in which personal information is stolen and used by criminals to begin a new life posing as the victim. The objective of this type of crime is for the criminal to escape their current identity and their past history. Criminals responsible for these types of crimes use the stolen identity to apply for jobs, rent apartments, lease cars, establish services and utilities, and even open lines of credit which they maintain in good status. Some of the types of people involved in the crimes of identity cloning include: terrorists; illegal aliens; pedophiles; child abductors; criminals with arrest warrants; victims of abuse; people with troubled work histories; and people with adverse credit histories.

Business identity theft is similar to financial ID theft with the exception that the victim is a business instead of an individual. Criminals involved with these types of crimes often use stolen information to obtain credit cards or lines of credit in the name of the business. They can also use the information to obtain services or merchandise at the expense of the business. Further, they can impersonate the business to defraud the business' customers and clients. This can be devastating to the reputation of the victimized business.

Personal Information

The most critical information required to carry out these types of identity theft crimes are a person's full name, Social Security number and date of birth. With these three pieces of information, someone can obtain credit cards, loans, access existing bank accounts, open new bank accounts, and perform various other types of fraud. Other personal information often targeted by criminals includes: home address; phone number; e-mail address; bank account numbers; credit card numbers and expiration dates, current employer, address of employer; title; salary; driver's license number; state and city of birth; mother's maiden name; passwords; and pin numbers.

There are many methods widely in use today to steal personal information. These attacks on confidential data can be extremely high-tech, involving the latest technologies and most recent security exploits. Many of the attack methods, however, are very low-tech, involving little or no technology at all. By taking a detailed look at the various types of attacks, it should become clear that private information is constantly at risk. A prudent defense strategy begins with awareness. While explicit countermeasures to these attacks will be discussed, it is important to remember that the first step is an understanding of the threats. Knowledge of these types of attacks leads to alertness and cautiousness in everyday activities, which is the foundation of a sound security plan.

Social Engineering Phone Attacks

The term "social engineering" is often used, in regards to information security, to describe a hacker's manipulation of a person in order to obtain information that would permit unauthorized access to a computer system. However, the term

© SANS Institute 2005 Author retains full rights.

really has a broader meaning which describes any circumstance in which an attacker uses social skills to deceive someone into revealing sensitive or confidential data. There are many ways in which social engineering is used to obtain personal information for the purposes of identity theft.

Several months ago my brother received a phone call from a man who stated that he was calling from E*Trade because there was an overdue charge of $6.00 on my brother's account. The caller explained that the phone call was a courtesy and that he would be happy to accept a payment by phone in order for my brother to avoid a late payment fee. My brother did have an E*Trade account, but he knew that it hadn't been used in a long time and that there should be no reason for a $6.00 overdue charge. He became suspicious of the call and replied to the caller that he appreciated the information but he would need to call E*Trade back to confirm the charge before making any payments. The caller insisted that wasn't necessary and reiterated that a payment could be made over the phone in order to avoid additional late fees. My brother ended the call without providing any information to the caller and immediately called E*Trade to inquire about his account. The response he received was that there was no overdue charge on his account and that no one from E*Trade had contacted him. This was clearly a social engineering attack by phone. Had my brother trusted the caller, he would no doubt have been asked to provide personal information in order to settle the bill. Most likely this would have included his E*Trade account number, his credit card number, his address and phone number, and possibly information such as his Social Security, mother's maiden name, and E*Trade password.

Another example of a social engineering phone attack is a caller that claims to be from Visa, or another credit card company, calling to confirm suspicious charges on the person's credit card. The attacker describes fictitious charges (unusual charges that would seem suspicious to a credit company) and hopes that the victim, not recognizing the charges, believes that their credit card number has been compromised and that someone is making charges on their account. If this attack succeeds, the victim will state that the charges are fraudulent and the attacker will respond by offering assistance in suspending the account and reversing the disputed charges. The attacker then attempts to gain personal information under the pretense that it is being used to verify identity. For example, this may be accomplished by phrasing requests in ways such as "in order to suspend this account and avoid more charges, will you please confirm your Visa account number?" and "before I reverse these charges, may I please have your Social Security number and date of birth in order to verify your identity?" In these examples, the attacker leads the victim to believe that he or she is already in possession of the request information and the victim doesn't realize that the information given in response to the question is actually being revealed to the attacker. Also, notice how in both examples the attacker incorporates their ability to help the victim into the request and makes the requested information a requirement for that help. This is classic example of

© SANS Institute 2005 Author retains full rights.

social engineering, with the attacker playing on the fears of the victim (being liable for fraudulent charges, losing access to credit lines, adverse effects on credit history, etc.) while assuming a position of trust and authority that can help the victim alleviate those fears (the credit card company that has the power to absolve the victim of financial responsibility for fraudulent charges) in order to obtain personal or confidential information without the victim even knowing that they were attacked.

Social Engineering Phone Attack Countermeasures

The best defense to these types of attacks is to never give out any information when receiving a phone call. It is not sufficient to trust caller ID to confirm the caller's identity, as there have been reports recently of the ability to spoof caller ID systems.[6] When personal information is requested during a received call, the best countermeasure is to do as my brother did and end the call without providing any information to the caller and then initiate a call yourself to confirm the request for information is legitimate. In doing this, it is critically important that you do not rely on the caller to provide you with a phone number to call back. The point of initiating the call is to assure that you are speaking with the proper business or organization, and this can only be accomplished when you obtain the number from a trusted source.

Phishing Attacks

Another form of social engineering comes in the form of fake e-mails and fraudulent websites designed to deceive people into revealing personal information. These types of attacks are referred to as "phishing". On September 22, 2004, the Deputy Assistant Director of the FBI, Steven Martinez, testified before Congress about the FBI's efforts to combat identity theft. During that testimony, Martinez identified phishing attacks as a crime problem which the FBI recognizes and discussed a special project being undertaken jointly by the FBI and other government agencies to specifically address phishing. In defining phishing to Congress, Martinez stated:

> Phishing schemes have a consistent nexus to Identity Theft. Phishing is the creation and use of fraudulent but legitimate looking e-mails and web sites to obtain Internet users' identities and financial account information for criminal purposes. Internet users, who believe they have received an authentic solicitation for information from an entity with which the user has a trusted relationship, are duped into providing their sensitive personal information to criminals who have "spoofed" the e-mails and web sites of the trusted companies and/or government agencies with whom the victims believe they are interacting. The most frequent targets of interest for

[6] "VoIP Hacks Gut Caller ID." July 6, 2004.
URL: http://www.securityfocus.com/news/9061 (October 2004)

© SANS Institute 2005 Author retains full rights.

criminals conducting such attacks are web sites belonging to the financial services sector, ISPs, and on-line auction venues.

Criminals who engage in Phishing often employ spamming (mass e-mail) techniques to send the Phishing e-mails to thousands or even millions of potential victims nearly simultaneously. Thus, Phishing can be a lucrative criminal enterprise even if only a small percentage of the recipients are deceived into disclosing their personal financial and/or other sensitive information.[7]

A recent example of this type of attack is the distribution of a fake e-mail circulating that was an imitation of a solicitation by the Kerry-Edwards campaign. The fake e-mail was a slightly edited version of a real e-mail distributed by the Kerry-Edwards campaign and pointed potential contributors to a fraudulent web page, located on a server in India, designed to accept payments. MSNBC reported that "aside from stealing money, the hoax's intent was to lure supporters of the Democratic ticket into becoming victims of identity theft."[8] This particular e-mail should have been recognized as a phishing attack, by the attentive recipient, because it contained misspellings found in the "from" and "subject" lines. This included president spelled as "presidewd" and decision spelled as "decesion". Misspellings are very common in phishing attacks and should raise suspicion when encountered in any e-mails or websites associated with a request for information. Examples of other real phishing attacks can be found at http://www.antiphishing.org/phishing_archive.html.

Phishing Attack Countermeasures

Be suspicious of any e-mail or website that requests personal information, especially in a context which requires an immediate response. Phishing attacks often employ tactics to create pressure to provide the information quickly. Also be attentive to misspellings and misuse of language in e-mails and websites as these are common in phishing attacks and often indicative of fraud. If you are unsure of the legitimacy of an e-mail, contact the company by phone, using a trusted number, to confirm that the e-mail is authentic. Remember that e-mail is not a secure means of communication, so personal information should never be sent via e-mail. This includes e-mails with specific forms for providing information. The exception to this is if encryption is used to secure the e-mail data. Avoid using hyperlinks included in e-mails, as they can display one address while actually linking to another. In addition, once connected to a fake site, there are ways that attackers can overwrite the URL in the address bar of

[7] "Testimony of Steven M. Martinez, Deputy Assistant Director Federal Bureau of Investigation, Before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census." September 22, 2004.
URL: http://www.fbi.gov/congress/congress04/martinez092204.htm (October 2004)
[8] Sullivan, Bob. "Kerry Donors Targeted By Fake E-mail." August 2, 2004
URL: http://www.msnbc.msn.com/id/5581739/ (October 2004)

© SANS Institute 2005 Author retains full rights.

the browser to display a fake URL. So it is not sufficient to simply read the address in the address bar of the browser, after using a hyperlink, as a means of confirming the site to which you are connected. Also, be wary of addresses which contain the "@" symbol. This symbol in a URL is used to specify a specific user for a site, in the format http://user@domain. However an attacker may specify the user portion as the name of a legitimate site in order to fool the uninformed victim. An example of the would be the address "http://www.ebay.com@1.2.3.4", which may appear, to an unaware user, as an address for eBay.com, but which actually links to a server at the address 1.2.3.4 with the username "http://www.ebay.com". Another means of misdirection in address names is for an attacker to use an address such as "http://www.ebay-members-security.com" or "http://www.mycitibank.net" which may appear to be legitimate but which are not registered addresses of the implied companies. These two examples were actually used in known phishing attacks and are, of course, not addresses affiliated with eBay or Citibank. A more secure alternative to using hyperlinks is to open a browser and connect to a site by typing the company's address into the address bar.

Malware and Spyware Attacks

Malicious software, often called malware, encountered in the form of viruses, worms, and Trojan horses can often expose confidential information. Viruses and worms have the ability to self replicate, viruses by attaching themselves to other programs and worms by propagating themselves, often by exploiting the file transfer capabilities of systems. Trojan horses are programs disguised as legitimate software but which include harmful code that is hidden from the end user. Most viruses and worms exploit know vulnerabilities in software and operating systems. New malware is being created every day and much of it is designed to compromise system security and grant attackers access to protected systems and information. For example, today October 18, 2004, as I reviewed this paper, a worm called "W32.Spybot.FBG" was discovered. According to Symantec it "includes distributed denial of service (DDoS) and back door capabilities. The worm also attempts to steal confidential information from the infected computer."[9] Also discovered today, a worm called "W32.Darby.B" which, in addition to other malicious activity, searches for cached passwords to send out via e-mail and attempts to disable anti-virus and firewall software.[10] Malware that monitors computer activity, without the user's knowledge, is referred to as spyware. This invasive software often captures and logs computer activity, such as e-mails, chat-sessions, internet connections, and in the worst cases includes keystroke logging; a complete record of everything the victim types on the keyboard, which can include user names, passwords, credit card numbers, and other personal information. Spyware often gets installed via a Trojan horse,

[9] URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.fbg.html (October 2004)
[10] URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.darby.b.html (October 2004)

© SANS Institute 2005 Author retains full rights.

when a victim downloads and installs freeware from the Internet and doesn't realize that the installation of the program also includes the malicious spyware code.

Malware and Spyware Attack Countermeasures

Assure that systems are continually maintained with current patches and security fixes. This includes not only updates for the operating system but also updates for installed applications. Always run anti-virus software with current virus definition signatures. Assure that the anti-virus software includes real time monitoring of files as they are accessed. Most anti-virus software includes the ability to update the signatures automatically. Schedule this update to occur daily, at a time that the system is usually powered on and connected to the Internet. Verify periodically that the auto-update feature is working and the signatures are being updated. Use an up-to-date personal firewall. Maximize security settings in all software. Disable features in operating systems and applications if they are not needed, such as HTML e-mail, instant messaging and file/print sharing. Do not use an e-mail preview pane that allows viewing attachments automatically, as this could execute malware. Run anti-spyware software, such as Lavasoft's AdAware or McAfee's Antispyware. Encrypt personal information stored on your system and all sensitive e-mails. Avoid using public computers to communicate any personal or confidential information. If you are required to use a public computer or someone else's computer for these purposes, consider booting the system to a bootable OS from CD such as Knoppix[11]. Keep in mind that while an OS like Knoppix will be effective in circumventing any malware that may have been installed on the system, it will not provide protection against a physical keystroke logger, which is a small device that can be attached between the keyboard and computer to record all keystrokes onto a memory chip. An attacker can place a physical keystroke logger on a public computer and then return after a period of time to collect the device and the stolen information. Only download and install software from trusted sources and avoid opening executable files received via e-mail.

Credit Card Number Hacking Attacks

In addition to compromising systems through malware, attackers often hack systems in order to steal information; a primary target for these attacks is credit card numbers. By exploiting security vulnerabilities attackers are often able to penetrate systems and steal information such as credit card numbers. In February of 2003, CNN reported that Data Processors International, a company that processes credit card transactions on behalf of merchants, experienced an in intrusion in which a hacker was able to obtain millions of credit card numbers. "MasterCard estimated that the hacker may have gotten access to information on as many as 8 million credit card accounts overall, including 2.2 million of its own

[11] For more information about Knoppix see:
URL: http://www.knopper.net/knoppix/index-en.html (October 2004)

© SANS Institute 2005 Author retains full rights.

cards. Visa said 3.4 million of its cards were affected"[12] Credit card information is at risk to these attacks when merchants and businesses collect credit card information in order to process transactions but then fail to store the information securely. Every time you provide your credit card number to a merchant that stores it, you add your information to another system and you increase your exposure to these types of attacks.

Credit Card Number Hacking Attack Countermeasures

An effective countermeasure to avoid having your credit card number compromised while being stored by a merchant is to use temporary numbers when shopping. MBNA has a program called *ShopSafe* that allows its customers to go to a secure website and generate a new credit card number with a specific credit limit and expiration date for each purchase. This way if you want to make a $129 purchase, you can create a unique credit card number with a credit limit of only $129. Once you provide the number to the merchant and the card is charged, it doesn't matter if the merchant stores the number or if the number is compromised in the future because after the initial charge it will no longer be a valid number. Other credit card companies offer similar services, such as Citibank's *Virtual Account Numbers Program* and Discover's *Deskshop Virtual Credit Card.*

Skimming Attacks

Skimming is the unauthorized reading and storing of information from the magnetic stripe of a credit or debit card. These attacks can occur when someone that has physical access to a credit card for a legitimate charge, such as a waiter or cashier, makes an additional swipe of the card through a small reader device known as a skimmer. The personal information contained on the magnetic stripe is captured and recorded by the skimmer and can then be used to create a counterfeit card or to make fraudulent purchases. Another form of this attack occurs when a legitimate payment terminal or ATM is tampered with, through altered software or hardware, to include skimming capabilities. When a card is swiped through the compromised system, the information on the card is stolen.

Skimming Attack Countermeasures

Watch carefully what is done with your card when you give it to anyone to make a charge. At restaurants, avoid giving your card to a waiter at the table to take away for processing. Instead, if possible, pay where the credit card machine is located so that you can keep an eye on your card. Be aware that skimmer devices are very small, often the size of a pager or small cell phone, and can be easily concealed. It only takes a couple of seconds to swipe a card through a

[12] "Hacker Hits Up to 8M Credit Cards." February 27, 2003
URL: http://money.cnn.com/2003/02/18/technology/creditcards/ (October 2004)

© SANS Institute 2005 Author retains full rights.

skimmer. Try to only use ATMs at well know banks and avoid using ATMs at places such as convince stores, gas stations, bars and restaurants; as these locations are more likely to be compromised.

Personal Theft Attacks

Anywhere personal information resides is a potential target of identity theft attacks. The US Postal Inspection Service protects the mail system from misuse and is very involved in crimes related to identity theft.

> Postal Inspectors investigate cases of identity theft because much of the criminal activity takes place through the mail. Mail may be stolen to obtain the information needed to apply for checks credit cards or to complete fraudulent applications for new cards. Financial institutions mail checks or credit cards that may be stolen by crooks, who can use anonymous addresses at commercial mail receiving agencies (CMRAs; also called "mail drops") to collect the proceeds of their crimes.[13]

A great deal of personal information is often sent and received via the postal system and most of this mail spends a period of time in unsecured personal mailboxes. In addition to stealing mail from mailboxes, attackers will often look through people's trash and the trash of businesses for personal information that has been discarded. Even personal information within your house may be vulnerable to guests and visitors, when not properly secured. Wallets and purses have long been the target of theft for money and credit cards, but are now also being targeted for the personal information they contain.

Personal Theft Attack Countermeasures

Use a home mailbox with a locking mechanism or a secured post office box located at a US postal office to receive mail. Never place outgoing mail in an unsecured mailbox; always bring it to a post office or place it in a secured official US postal mailbox. Remove mail from your locked mailbox as soon as possible and be sure to stop or forward mail when you plan to be away for extended periods of time. When ordering checks, be sure to have them sent to your home via registered mail. Frank W. Abagnale, a reformed thief and respected authority on identity theft, recommends these two important steps to reduce the amount of mail received that includes personal information:

> Remove your name from the marketing lists of the three credit reporting bureaus to reduce the number of pre-approved credit offers you receive. Add your name to the name-deletion lists of the Direct Marketing

[13] URL: http://www.usps.com/postalinspectors/fraud/IdentityTheft.htm (October 2004)

© SANS Institute 2005 Author retains full rights.

> Association's Mail Preference Service and Telephone Preference Service used by banks and other marketers.[14]

Shred anything that contains personal information of any kind using a cross cut shredder before disposing of it in the garbage. Remove and shred labels containing personal information from boxes and containers prior to putting them out in the garbage. Always secure identifying receipts and shred them prior to disposal. Avoid leaving documents around the house that contain personal information, such as mail, financial records, and medical records. Instead secure this information in a safe place such as a locked drawer or cabinet. Don't carry more identification than is necessary and also don't carry more credit cards than are necessary. Be mindful of people looking over your shoulder when using an ATM, a phone card, or a credit card. Never carry your social security number with you (including in your wallet or purse). Social security numbers should be treated with the utmost protection. The US Social Security Administration provides the following advice regarding your Social Security number:

> You should be very careful about sharing your number and card to protect against misuse of your number. Giving your number is voluntary even when you are asked for the number directly. If requested, you should ask:
>
> - Why your number is needed;
> - How your number will be used;
> - What happens if you refuse; and
> - What law requires you to give your number
>
> The answers to these questions can help you decide if you want to give your Social Security number. The decision is yours. [15]

Review the privacy policies of any business, organization or group that you conduct financial or medical business with and assure that they are taking appropriate measures to safeguard your personal data. The privacy of personal data held by financial institutions is protected under the Gramm-Leach-Bliley Act[16] and the privacy of personal medical data is protected under the Health Insurance Portability and Accountability Act.[17]

Detection and Response

---

[14] Abagnale, Frank. "14 Tips to Avoid Identity Theft." July 15, 2004
URL: http://www.bankrate.com/brm/news/advice/20030124b.asp (October 2004)
[15] "Your Social Security Number and Card." July, 2004.
URL: http://www.ssa.gov/pubs/10002.html (October 2004)
[16] For more information about the GLB Act see:
URL: http://www.ftc.gov/privacy/glbact/ (October 2004)
[17] For more information about HIPPA see:
URL: http://www.hhs.gov/ocr/hipaa/ (October 2004)

© SANS Institute 2005 Author retains full rights.

Early detection of the crimes of identity theft by the victim is critical in minimizing damages. The best method of detection is to keep a careful eye on your credit report. Credit reporting services such as TransUnion's *TrueCredit ID Fraud-Watch* provide notification services of any changes to credit reports as well as access to full reports several times a year. A real time notification of changes to your credit report is an ideal detection strategy. At a minimum your credit report should be carefully reviewed twice a year. In addition, it is important to review all existing financial accounts for accuracy in a timely manner at the close of each billing cycle. Be alert if financial statements fail to arrive when you expect them, as this could be an indication that someone has changed the address on your account. If fraud is detected, the Federal Trade Commission recommends placing a fraud alert on your credit files with any one of the three major credit bureaus, closing all accounts believed to be compromised, filing and obtaining a police report, and filing a complaint with the FTC. This process is explained in more detail at the FTC ID Theft website located at http://www.consumer.gov/idtheft/recovering_idt.html.

Conclusion

Your identity is yours to protect. By understanding how identity theft attacks occur and the countermeasures used in defense, you are empowered to take the actions necessary to secure your personal information and protect yourself against these very serious crimes.

© SANS Institute 2005, Author retains full rights.

References

"Federal Trade Commission – Identity Theft Survey Report." September 2003
URL: http://www.ftc.gov/os/2003/09/synovatereport.pdf (October 2004)

"President Bush Signs Identity Theft Penalty Enhancement Act." July 15, 2004.
URL: http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html
(October 2004)

"Identity Theft and Assumption Deterrence Act of 1998."
URL: http://www.identitytheft.org/title18.htm (October 2004)

URL: http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm (October 2004)

URL: http://www.idtheftcenter.org/cresources.shtml (October 2004)

"VoIP Hacks Gut Caller ID." July 6, 2004.
URL: http://www.securityfocus.com/news/9061 (October 2004)

"Testimony of Steven M. Martinez, Deputy Assistant Director Federal Bureau of Investigation, Before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census." September 22, 2004.
URL: http://www.fbi.gov/congress/congress04/martinez092204.htm (October 2004)

Sullivan, Bob. "Kerry Donors Targeted By Fake E-mail." August 2, 2004
URL: http://www.msnbc.msn.com/id/5581739/ (October 2004)

URL:
http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.fbg.html
(October 2004)

URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.darby.b.html
(October 2004)

URL: http://www.knopper.net/knoppix/index-en.html (October 2004)

"Hacker Hits Up to 8M Credit Cards." February 27, 2003
URL: http://money.cnn.com/2003/02/18/technology/creditcards/ (October 2004)

URL: http://www.usps.com/postalinspectors/fraud/IdentityTheft.htm (October 2004)

© SANS Institute 2005 Author retains full rights.

Abagnale, Frank. “14 Tips to Avoid Identity Theft.” July 15, 2004
URL: http://www.bankrate.com/brm/news/advice/20030124b.asp (October 2004)

URL: http://www.antiphishing.org/consumer_recs.htm (October 2004)

URL: http://www.csoonline.com/read/090104/briefing_phish.html (October 2004)

Bruce, Laura. “Skimming the Cash Out Of Your Account.” March 26, 2003
URL: http://www.bankrate.com/brm/news/atm/20021004a.asp?prodtype=bank
(October 2004)

Lazarony, Lucy. “On The Dark Side of Credit Card Fraud.” May 24, 2002
URL: http://www.bankrate.com/brm/news/cc/20020524a.asp

URL: http://www.fraudwatchinternational.com/frauds_and_scams/skimming.htm

URL: http://www.consumer.gov/idtheft/

URL: http://www.usdoj.gov/criminal/fraud/idtheft.html

© SANS Institute 2005, Author retains full rights.

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event