Global Information Assurance Certification Paper

Identity Theft and Information Security

By

Mike McCarrier

GSEC Practical Assignment 1.4b

Option 1

Date Submitted: 06/18/2004

Identity Theft and Information Security

Abstract

Identity Theft and its relationship with Information Security is becoming a point of discussion within the IT security community. This paper discusses the various issues raised by Identity Theft. Among these issues are certain methods that are utilized by perpetrators of Identity Theft. Increasingly, these methods involve the use of computers and other electronic devices.

Those involved with IT security now have to include Identity Theft as a prevalent risk. Also discussed, is how an individual or business can mitigate these risks and protect themselves. Being aware of the risks is often the first step to preventing intentional or unintentional disclosure of personal information. By using security tools that are readily available through the Internet or retailers, businesses and individuals can help protect their identity from falling into the wrong hands.

Introduction

The Information Age has provided us with new and unique advancements to help make our lives easier. One of the improvements the Information Age has brought consumers is the ability to shop on-line. With a few short clicks, a consumer can buy almost any product and have it sent right to his or her doorstep. Stores that do not have a physical presence in a particular city, region, or country can sell to people from around the world.

However, there is a risk associated with conducting business on-line. The added convenience of shopping on-line can allow certain dishonest individuals to take advantage on-line shoppers. If on-line shoppers are not careful, they can have their credit card number or even their identity stolen from them in a matter of minutes. The result is a reduced sense of consumer confidence in on-line retailers and businesses.

Many businesses these days are shifting their selling strategies to the world-wide web. Businesses include E-Mail as a medium of advertising, site statistics so businesses can better serve their customers, and even small programs called cookies to track which users have visited their web site to effectively manage their web based store fronts. Some companies are solely, “E-Sellers” or businesses that conduct most or all of their business over the Internet. This trend is affecting the way information security is handled and implemented. With much at stake for consumers and business alike, it is no wonder why information security is a hot topic in the world of “E-Business”.

Through careful planning and diligence, consumers can learn to protect themselves from identity theft. By keeping informed of the issues and technologies to combat identity theft, on-line shoppers can prevent their personal information from falling into the wrong hands. This helps reduce the anxiety and uncertainness of on-line shopping and allows Internet users to fully enjoy their on-line experience.

The Definition of Identity Theft

Identity theft is a crime in which an imposter obtains key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen (searchSecurity.com, 2002).

The scary part is this information can be easily obtained. If a criminal wants someone's personal information, then they will do anything to get it. This can include looking for old computers or discarded hard drives and floppy disks in the garbage. This can have a negative impact on both businesses and individuals. What many businesses and individuals do not realize, is that a thief can use available tools found on the Internet or underground web sites and recover personal information from hard drives and floppy disks. This information can include credit card numbers, check numbers, and driver's license numbers. Just deleting a file on your computer does not mean it is erased from the hard drive.

What this means for businesses is the potential theft of confidential or propriety information. This information could be employee and customer social security numbers, trade secrets, and memos between company employees. Businesses have to view the theft of confidential information seriously. Not only are there legal ramifications, but a company's integrity and reputation can be tarnished. Customers may not trust certain businesses once they hear of identities and information being stolen. The process to win back the trust of these customers can be tough.

Individuals have just as much, if not more to lose, as businesses do. Credit ratings can be ruined, bank accounts pilfered and drained, and countless time has to be spent correcting and having erroneous information removed from credit reports and records. The first step usually involves the victim convincing a bank or credit institution that he or she is a victim of identity theft. Unless the victim has proof of their transactions, such as receipts, then it is hard to convince a credit card company or other financial institution that he or she does not owe them money (Crimes of Persuasion.com).

Identity Theft in the News

As Identity Theft becomes more prevalent, so does media coverage of it. This can serve consumers and businesses in a positive way. Identity Theft can happen to anyone and warning the public is not enough. Reading and watching news about Identity Theft is a value tool. It can make some people more cognizant of it and prompt them to be more careful with their personal information.

According to a recent article on eWeek's website, "reports of Internet-related fraud now account for more than half the consumer complaints filed with the Federal Trade Commission" (McDonough, 2004). Of those complaints, Internet auctions represented 15 percent of the complaints, while shop-at-home/catalog sales were 9 percent, and Internet services and computer complaints made up 6 percent (McDonough, 2004). This does not represent a headache for consumers only, but for online retailers as well. Especially given the legitimate nature of most web sites.

EBay, for example is a popular online auction site where sellers can put items up for bidding. Buyers only need to submit a bid with a click of a button. Therein the problem lies, there is not a way to know if a seller is reputable. Imagine ordering food in the drive-thru of a fast-food restaurant. After the order is placed, the customer drives up to a window to receive it. Once the payment is received, the customer receives his or her order. What if that order is a hamburger instead of a cheeseburger? By time the customer realizes that they did not get what they paid for, they are usually at home about ready to eat.

Internet-related identity theft can also be perpetrated through E-Mail. A story posted on KATU-TV provides a case where a legitimate businesses' identity was stolen. America Online customers received authentic-looking e-mails claiming there was a billing problem with their AOL account and asking them to update their information or risk losing Internet access. The message included a link to an "AOL Billing Center," a fake Web page dressed up with the company's logo, colors and links to real AOL sites (Ho, 2003). All the perpetrator did was use America Online's intellectual property, and was able to obtain personal information.

Imagine if the personal information and identities of close to 200,000 people were compromised. It happened to San Diego State University. A server in the financial aid office was intruded by hackers. The intruders had access to the server beginning in late 2003 and continuing until the end of February 2004 (Identity Theft 911, 2004). The worse aspect of this intrusion is that university officials did not know if personal information was stolen and were not aware any intrusion took place.

The San Diego State University computer intrusion incident further highlights a worry from tech companies and vendors: consumers lack knowledge to protect themselves (Kumler, 2004). Spyware, for instance can degrade the performance of a computer's network connection. Small programs send information back and forth to spyware manufacturers with information containing, but not limited to, the computer user's activities. Manufacturers of spyware use this information to market products (Pop-Ads and/or web site advertisements) and/or sell the information to other businesses and individuals. While the information that is transmitted to the spyware makers may be trivial in nature, such as web sites a user has visited, the software itself can annoy users. Some users may blame the problem on their computer or Internet connection. As a result, customers call the manufacturer of their computers or Internet Service Provider. The time spent finding and correcting the source of the problem can be costly to businesses in terms of money. Unless the customer is convinced the

problem was a result of spyware, the reputation of a computer manufacturer or Internet Service Provider may be damaged.

How does Identity Theft happen?

This section will describe a typical Identity Theft incident. The scenario described is a fictional story. This story is related to what may happen when businesses and individuals become victims of Identity Theft. In the next section, the various methods of Identity Theft are described in detail.

Our scenario involves Mr. Average. He lives in a middle-class neighborhood with his wife and two kids. One day, Mr. Average is checking his E-Mail. He receives a statement from his local bank proclaiming that he is eligible to receive an extra $500 toward his savings account. He only needs to click on an icon in the E-Mail to receive his reward. The icon is exactly the same as the logo of the local bank. Convinced that the E-Mail messages is legitimate, Mr.Average click on the icon. He is taken to a web site that looks exactly like the local bank's. He is presented with a form in which to enter his banking information. He clicks the submit button and $500 is going to be deposited to his bank account. Or will the money not be deposited?

Later in the week, Mr.Average receives his bank statement in the mail. After examining it, he finds something peculiar. It says that $500 was withdrawn from his account. Convinced that there has been a mistake, Mr.Average contacts his local bank. Mr. Average explains that he received an E-Mail from the bank claiming that he was eligible for extra $500 towards his savings account. The customer representive fielding Mr.Average's call explains that no such E-mail was sent to the bank's customers. Mr. Average was tricked into giving someone other than the bank his savings account number.

It turns out, a clever computer expert stole copyrighted material from the website of the bank Mr.Average does business with. The computer expert used logos and graphics to make the E-Mail message seem legitimate. When Mr. Average was directed to a web site that looked exactly like the website of his bank, he thought there was nothing wrong. What many computer users do not examine, is the web address of a particular site. There are many web sites that have links to other sites owned by the web site owner. The web address may be different, but the look and design is fundmentality the same. A clever criminal can trick a computer user into giving them personal information by the use of an input box or form. Instantly, the criminal has the personal information of an unsuspecting person.

Methods and examples of Identity Theft

The identity theft method employed against Mr. Average is one of many methods used by identity theft perpetrators. In this section, the various methods employed against victims of identity theft are discussed. The sophistication of these techniques ranges from a simple phone call to malicious software. A few of the methods discussed can be used in combination with other methods of network

and computer intrusion. The purpose of these methods are the same; to get personal information

The method employed against poor Mr. Average included a fake website. Imagine sending a letter to a person with a fake name. The address may be correct, but the name on the envelope is not. As a result, an unsuspecting victim could be sending a check or personal information to this unknown person. A fake website functions in much the same way. A fake website assumes the identity of a legitimate business, such as Wal-Mart or Ebay. Users that visit a fake website could be elicited to provide confidential or private information such as bank account numbers, credit card numbers, and/or Social Security numbers.

A fake website soliciting personal information is described by PCWorld columnist, Steve Fox (Fox, 2003). Job search and resume sites help connect potential employees with employers. Prospective job candidates can send as many resumes as they please to answer job postings on the Internet. However, this presents an opportunity for criminals to fraudenantly assume the identity of a legitimate job search website and steal personal information. These criminals can go a step further and sell information from the resumes to the highest bidder. Worse yet, a person's resume could be stolen and used by the criminal in a job search.

Key loggers are software or hardware with a dual purpose. They record every keystroke entered by a user on a computer keyboard. When used properly, a key logger can provide valuable information to monitor the activities of company employees or suspected criminals. However, key loggers can be used with bad intentions, especially if the victim is not aware that key logging software exists on his or her computer.

The use of a key logger for criminal intentions, involves 19-year old Van T. Dinh (Roberts, 2003). Dinh was accused of committing identity theft in addition to charges of computer hacking. The actions of Dinh were out of desperation. He owned 7200 shares of Cisco stock options that were deemed worthless. As owner of the stock options, Dinh was allowed to sell the options at or below $15 a share before July 19, 2003. Dinh would have had to take a loss of nearly $40,000 if he decided to sell his stock options.

Dinh formulated a complex plan to unload his stock options without taking a loss. He lured users of an on-line stock discussion group into downloading a key logger he claimed was a stock charting tool. Once the user downloaded and installed the key logger, Dinh was able to steal user names and passwords for TD Waterhouse Investor Services online brokerage accounts. He then made bogus transactions by selling his stock options and then executing buy orders using the stolen online brokerage accounts. Unsuspecting victims were bilked of nearly $50,000.

Phishing is a method of Identity Theft which uses known logos from entities such as PayPal, eBay, and America Online (Rubenking, 2004). A victim of Phishing usually receives a legitimate-looking E-Mail that contains a message to trick the user into giving personal information. Often, this message is described as 'Urgent' or 'needs attention'. Once the user clicks on the logo or link contained in the E-Mail message, he or she is directed to a web site. Once

the user is redirected to the web site, they are asked to enter information in a form or input box. Perpetrators of Phishing are clever enough to take the website down, once it has served its purpose. The result is a fly-by-night operation, which makes the task of catching the criminal responsible a tough task.

Grey Todd is one victim of Phishing (Rubenking, 2004). Todd received an E-Mail proportedly from PayPal related to an old company E-mail account. The E-Mail elicited him to enter personal information, such as his Social Security Number and ATM PIN. After this event, Todd grew suspicious and reported to PayPal that he had been scammed.

Spyware is any technology that aids in the gathering information about a person or organization without their knowledge (Techtarget.com, 2004). Sometimes spyware can be manufactured for legitimate means, such as tracking certain web sites a user has visited. In other instances it can be installed for mining or stealing confidential information. If the user is aware that software will be installed to record information, what that information is, and what companies, if any, will his or her information be shared with, it is not considered spyware. If the software manufacturer does not disclose that data or information collecting software will be installed, then it is considered spyware. The definition of spyware as defined by law is a constant point of debate. There are some companies that use information gathering technologies responsibly and do not allow other companies to obtain information from them. However, there are a few companies that chose to ignore the privacy of individuals and are willing to collect information that they do not have a right to process.

Spyware can take the form of cookies, which are small programs, or viruses and worms. Still others can be stand alone programs that are installed without any user interaction. Spyware functions by transmitting information back to the software manufacturer. Many companies use this information to design web sites based on the amount of traffic that is being received, what time of day most users access the site, what areas of the site users are accessing, etc. However, it can allow the exposure of user information that is considered private. Spyware can open up ports, such as those accessed by file sharing software, and allow a malicious user to place viruses and worms on someone's computer. Other spyware simply searches for credit card numbers, social security numbers, and passwords for use in identity theft or unauthorized access to a computer.

Social Engineering, in relation to Information Security, is the process of extracting information, usually through verbal means, from an individual in order to gain access to a secure location and the information contained within (Granger, 2001). The secure location could be, for a example, a building, computer, or storage area for confidential documents. One of the more common methods of Social Engineering involves a typical phone call. The victim is usually tricked into giving out sensitive information, such as a password, to an unauthorized person. Social Engineering culprits will make the victim believe that he or she is a trusted person, such as "Jack" or "Jill" from IT support services. Like another method of Identity Theft, Phishing, the victim is often given a legitimate reason for given out the requested information, usually having to do with an "urgent" or "important"

event. The result is a Social Engineering perpetrator obtains information to circumvent security measures.

Hardware weakness is the lesser known of Identity Theft Methods discussed in this section. However, it rivals the techniques the movie goers often see when watching "James Bond". In fact, such hardware vulnerabilities are used to the advantage of government agencies, such as the Federal Bureau of Investigation and the National Security Agency. One such hardware weakness is TEMPEST emanations (Rittenhouse, 2002). TEMPEST emanations are electronic signals created by a computer monitor. These signals can be used to recreate computer screen images with sophisticated reception equipment. This method of information gathering does have one shortfall, the computer monitor being targeted must be in close proximity to reception equipment. Such equipment is illegal to possess in the United States. The likelihood of this method being employed against ordinary individuals is minimal. A person would have to be high on the government's watch list in order for such a method to be used against him or her.

Many computer owners do not realize the value of computer sanitization. To them, a file that has been deleted can not be recovered. When it comes time to buy a new computer, it is not uncommon to see an old computer lying in the garbage. However, a skilled individual can utilize a variety of data recovery tools to steal information from computer hard drives and other storage mediums that have been discarded or allocated for another use. This presents a threat to individuals and businesses that house confidential information on computers.

One example of the consequences of not sanitizing a computer hard disk was experienced by the United States Veterans Administration Medical Center. In August 2002, 139 computers owned by the United States Veterans Administration Medical Center were retired. The retired computers were donated or sold to other individuals and organizations. Some computers were found to contain confidential information, such as credit card numbers and the names of veterans with AIDS or mental health problems (Garfinkel and Shelat, 2003). By failing to properly sanitize confidential information, very personal information was inadvertently disclosed.

Solutions for Protecting Individuals and Businesses from Identity Theft

Secure transactions are a necessity when shopping online. It is in the best interest of companies to provide the ability to encrypt and secure sensitive data that their customers might transmit when shopping on their web sites. Internet browsers such as Microsoft's Internet Explorer, include the ability to accept and use encryption technologies. To check or verify that that a connection is encrypted, all a user needs to do is look for a padlock that is displayed in the desktop system tray (Learn The Net, 2004).

Digital certificates are another way to protect a consumer's identity. They also are good way for businesses to provide protection to their users from Identity Theft. When a user connects to a secure website, they receive a digital certificate. The recipient's web browser creates a session key to encrypt any

data that is transmitted between the website and user. The data is encrypted using the web site's public key, which is unique to the website. The website then decrypts the data transmitted to it using its own public key (Netscape, 2000). If the digital certificate were to be tampered with or compromised, the certificate can be revoked to prevent another website from using it and assuming a businesses' identity.

Spyware detection tools are helpful in allowing a user to remove or quarantine any software or programs that are transmitting information, confidential or not. Like other software detection tools, such as software that detects viruses, spyware detection tools look for known spyware programs and give the user an option to quarantine or remove the offending program (Metz, 2004). Spyware detection tools are only useful if the spyware program has been identified by its manufacturer. While, spyware detection software is less than perfect, it still is a good way to prevent spyware from harvesting a user's personal information.

Computers in public places can pose a serious risk of Identity Theft for its users. Airports, cafes, restaurants, and schools often provide access to users to check E-Mail or surf the Internet. Many of these computers do not employ technology to erase any trace of a user's activities. Potentially, a user could enter a password to a website that contains bank information and allow a malicious user to recover and use the user's authentication data. Products such as FSLogic Protect 1.0, discard user sessions and any information disclosing a user's activities once the user logs off (Rubenking, 2004). This protects the owners of publicly accessible computers from liability due to theft of personal information. Users can feel secure that their information will be safe. In an environment such as a school, each user's session is stored on a server after he or she logs off. Any information that resided on the computer during the user's session is transferred to a specific directory that can be unique to the user.

Anti-virus software is a must for anyone that owns a computer. Many viruses harm or destroy computer data. Some viruses are so damaging, that they can render a computer useless. Increasingly, viruses are being used to fool users into giving out personal or confidential information. Methods of Identity Theft, such as Phishing, can utilize viruses to evoke a program that prompts the user to enter information. The virus may find other E-Mail addresses on the victim's computer and spread itself to more users, as with the Minmail virus (Fisher, 2003). Having a good anti-virus program, such as Norton Anti-Virus or McAfee VirusScan, can help reduce the probability of a virus infection and also keep confidential information safe.

A hardware or software implementation of a firewall is a good idea when protecting against Identity Theft. The popularity of file sharing software such as Kazaa increases the chances that spyware and viruses are placed on a user's computer. Spyware and viruses can "piggyback" legitimate files such as Mp3's and infect a computer without the user's knowledge (Jaw's Computer Services, 2003). Spyware programs could try to open up connections to clandestine web sites and download viruses or other malware further damaging a computer. In some instances, key logging software can be downloaded threatening the

personal information of an unsuspecting user. Keystrokes and user activity can be transmitted to a malicious user and used to gain access to a victim's computer. If a user has confidential data housed on his or her computer, this information can be compromised and utilized for unlawful activities, such as unauthorized credit card purchases.

A firewall blocks illegitimate traffic from reaching a user's computer. Computer users and businesses have the option of implementing firewalls in software or hardware form. Some viruses and spyware try to open up connections using certain ports, such as FTP port 21. Firewalls can sense a connection request and prompt the user to allow or deny the connection. Firewalls can also be configured to run without the user interactively allowing or denying a connection attempt. Rules or filters can be applied to various ports and applications telling the firewall to deny or allow certain traffic. These rules and filters go a step further to allow or deny certain MAC or hardware addresses, and outgoing and incoming connections access to a computer.

Two-factor or multi-factor authentication can make the theft of personal information more difficult. In regards to a computer, it involves two or more methods of authentication, a password and either an encrypted token or biometric device to verify the user's identity. An unauthorized user may be able to crack a password to gain access to a computer, but since he or she does not have the correct access token and/or fingerprint, access is denied. A good example of two-factor authentication already in use, is using a badge or ID card to access a building and entering a password to access a computer (Coffee, 2003).

Identity Theft legislation is an important piece in protecting businesses and individuals alike that are or have been victims of Identity Theft. State and Federal governments have recently passed legislation that outlines the process for reporting an Identity Theft incident, rights an Identity Theft victim has in order to repair any damage caused, and the penalties that can be levied against an Identity Thief (Fight Identity Theft, 2004). An example of Identity Theft legislation is many states now require credit reporting agencies to freeze identity theft victims' credit records in order to prevent further damage to their credit. Along with other Identity Theft prevention measures, consumers can feel safer with the knowledge that certain laws exist to protect them. However, some users must realize that if an Identity Theft incident is perpetrated from outside the United States, then it may be subject to the laws of other countries. In that case, some countries do not have the resources or laws to prosecute Identity Thieves. Laws can only protect victims to a certain extent. Measures taken on the part of businesses and individuals to protect from Identity Theft are sometimes the best prevention.

Lastly, the simplest aspect of Identity Theft prevention is common sense. Everyone should know where their personal and confidential information resides and how it is used (Germain, 2003). This includes being aware of what information can or cannot and should not be shared. For instance, if a computer user is asked to enter his or her social security number while signing up for a free online newsletter, then alarm bells should be sounding in his or her head. A

person does not need to write down their social security number to buy a magazine subscription. The same should be said for online newsletters. In most cases, online newsletters do not require prospective subscribers to enter highly confidential information such as a social security number. In requesting information about a user, each website should have a privacy agreement that can be read and agreed upon by the user. That way, if there is any information that a user does not want to give out, then he or she has the right to decline the request. It also holds the web site owner responsible for how information is shared or used. If a website does not have a privacy policy or agreement, then a user should not buy items and signup for services or products as advertised by company represented. Simply put, the user could be dealing with an illegitimate web site or business. Businesses should make a point to develop privacy policies and agreements for their website users. This can help protect them from costly litigation procedures and damage done to their reputations.

Conclusion

Identity Theft can be a scary possibility to imagine. There are plenty of nice advantages to having an Internet connection and utilizing the many conveniences that it offers. A simple trip to an online store can save the stress and hassle of going to a crowded department store. Plus, with the busy lives many people have, it allows the convenience of shopping whenever one feels like it.

However, using a computer can scare some people none the less as they hear about hackers, and worms and viruses infecting computers in the media. With the various software makers that abound, computer users can have a hard time feeling that have invested in the right product. This can cause computer users to ignore security threats to their computers. They may feel that the time it takes to find a product that is easy to use and affordable is not worth the trouble.

Security measures to protect against Identity Theft are evolving to be less expensive and easier to use. The fact that some computer users lack technical expertise has made software developers more aware of the need to create products that everyone can use. The trick is to convince business managers and executives to approve these changes based on the money that will be saved mitigating security threats and risks. The break-even point may not be for awhile, but if the software is made right, the rewards speak for themselves.

Educating users about security risks and threats associated with Identity Theft is another piece that needs to be recognized. It is not enough to make software easy to use. All computers do not work the same and problems can occur. Allowing computer users resources to learn and apply security measures can help software makers better improve their products for future security risks regardless of who is using them. Something as simple as an E-mail address for software users to send questions and concerns can make a big difference. If a software maker can put the various terms and definitions in plain English, their users are more likely to understand security threats and risks. This is especially

helpful in order to maximize customer satisfaction and attract other customers that looking for information security solutions.

Ultimately, it is the consumers and businesses who will force software makers to become more cognizant of their software's vulnerabilities. Simply put, a security solution that is ineffective or hard to use is not going to be accepted by computer users and businesses who lack technical knowledge. This presents proverbial tradeoffs that are hard for software makers to get around. Chances are if a security solution is cheap, then it may not be secure enough. If a security solution is secure enough, it may not be cheap. Consumers and software makers must work together to create solutions that are relatively cheap and secure against most security risks and vulnerabilities.

List of References

1. "Identity Theft." *TechTarget*. 8 September, 2002. URL:http://searchsecurity.techtarget.com/sDefinition/0%2C%2Csid14_gci80187 1%2C00.html.

2. Germain M., Jack. "Identity Theft Online: Debunking the Myths." *TechNewsWorld*. 7 January, 2004. URL: http://www.technewsworld.com/story/32622.html.

3. "Schemes, Scams, and Fraud." *Crimes of Persuasion*. URL: http://www.crimes-of-persuasion.com/Crimes/Telemarketing/Inbound/MajorIn/identity_theft.htm.

4. Ho, David. "Officials: Internet identity theft is a growing problem." *Katu.com*. *21* July, 2003. URL:http://www.katu.com/consumernews/story.asp?ID=59279.

5. "SDSU Students and Staff at Risk of Identity Theft." *Identity Theft 911.* 17 March, 2004. URL: http://www.identitytheft911.com/education/article/20040317_sdsu.jsp.

6. Kumler, Emily. "Spyware's Victims Spread." *PCWorld*. 19 April, 2004. URL: http://www.pcworld.com/news/article/0,aid,115735,00.asp.

7. Fox, Steve. "Plugged In: Identity Scams Plague Career Sites." *PCWorld*. June 2003. URL: http://www.pcworld.com/howto/article/0,aid,110314,00.asp.

8. Roberts, Paul. "Hacker Busted for Identity Theft." *PCWorld*. 9 October, 2003. URL: http://www.pcworld.com/news/article/0,aid,112872,00.asp.

9. Rubenking, Janet. "Identity Theft: What, Me Worry?" *PC Magazine.* 2 March, 2004. URL: http://www.pcmag.com/article2/0,4149,1524396,00.asp.

10. *TechTarget*. 18 March, 2004. URL:http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci214518,00.html.

11. Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." *SecurityFocus*. 18 December, 2001. URL: http://www.securityfocus.com/infocus/1527.

12. Rittenhouse, David. "Privacy and security on Your PC." *ExtremeTech*. 28 May, 2002.
URL: http://www.extremetech.com/article2/0,1558,13921,00.asp.

13. Garfinkel, Simson L. and Shelat, Abhi. "Remembrance of Data Passed: A Study of Disk Sanitization Practices." *IEEE Security & Privacy, vol. 1, no. 1.* 2003.
URL: http://www.computer.org/security/v1n1/garfinkel_print.htm?SMSESSION=NO.

14. "Protect Yourself: Secure Transactions." *Learn the Net.com*. 5 January, 2004. URL: http://www.learnthenet.com/english/html/07secur.htm.

15. "Digital Certificates." *Netscape*.
URL: http://wp.netscape.com/security/techbriefs/certificates/.

16. Metz, Cade. "Spy Stoppers." *PC Magazine*. 2 March, 2004.
URL: http://www.pcmag.com/article2/0,4149,1523357,00.asp.

17. Rubenking, Neil J. "Safe Computing, Unsafe PCs." *PC Magazine*. 2 March, 2004.
URL: http://www.pcmag.com/article2/0,1759,1524367,00.asp.

18. Fisher, Dennis. "New Minmail Virus Poses as PayPal E-Mail." *eWeek*. 14 November, 2003.
URL: http://www.eweek.com/article2/0,4149,1383283,00.asp.

19. "On Spyware and Firewalls:" *JAW's Computer Services*. 4 November, 2003. URL: http://www.jawscomputer.com/IntSec.htm.

20. Coffee, Peter. "Making a Privacy Investment." *eWeek*. 21 April, 2003.
URL: http://www.eweek.com/article2/0,1759,1037026,00.asp.

21. *Fight Identity Theft*. 2004.
URL: http://www.fightidentitytheft.com/.

22. Germain, Jack M. "Identity Theft Countermeasures." *TechNewsWorld*. 7 October, 2003.
URL: http://www.technewsworld.com/story/31775.html.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event