Issues in Information Systems
Volume 14, Issue 1, pp.162-168, 2013

IDENTITY THEFT AND PREVENTIVE MEASURES: THE COST IS ALL YOUR'S

Joseph Compomizzi, Robert Morris University
Shana D'Aurora, Robert Morris University
Daniel P. Rota, Duquesne University

ABSTRACT

Despite the vast research on identity theft, little is known about the preventative measures of professionals who work in the information technology/systems sector who also instruct cyber security and information technology courses. The overall image that emerges from the literature is negative: lazy, corrupt, unpatriotic, apathetic con artists who will steal at all costs an individual's identity to use for their personal gain. This study recovers some of the low tech and high tech measures to safe guard one's self against identity theft. A quantitative survey was designed and distributed to information systems/security professionals teaching at a community college in the Eastern Panhandle of West Virginia. An analysis of the survey responses yields the information systems/security professionals own explanations of the methods used to safeguard their personal information from identity theft criminals. This study is part of a growing body of research on safe guard measures against identity theft. In researching professionals in the field who are also instructing course content on these same practices, this project will contribute to future research on similar topics of safe guarding one's identity.

Keywords: identity theft, cyber rings, identity fraud, identity theft, cloning, skimming and phishing

INTRODUCTION

Identity theft is defined as "knowingly transferring or using, 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" (U.S. Code, Chapter 47, Title 18, Section 1028(a)). In simple words, identity theft is when another person employs someone's personal identification information as their own. Its intent is to commit fraud or another crime. It causes lost job opportunities, denial of loans, loss of housing, and at the very minimum negative credit scores.

This article aims at providing definition, history, statistics, and information about how identity theft is committed and some measures that can be taken to avoid it based on primary research conducted at Blue Ridge Community and Technical College in Martinsburg, WV with instructors and professionals who work in information technology.

Defining Identity Fraud

As the Federal Trade Commission (FTC) (2012) explains, identity theft falls into three main categories: financial identity theft, criminal identity theft, and cloning. First, financial identity theft occurs when personal information such as credit card and social security numbers are obtained and enlisted with the purchase of goods and services. More common schemes of financial identity theft which go beyond the simple purchase of an item include credit card application, large purchases such as automobiles, and some cases reporting actions including the rental of apartments. On the other hand, with criminal identity theft, the thief employs the use of a citizen's identifying information for impersonation within the criminal justice system. This can happen with minor offenses such as traffic tickets. As well, cases where individuals have been impersonated and mistakenly convicted for felonies have been documented. At the extreme end of identity theft is cloning. Cloning is the total impersonation of someone. Cloning is assuming another person's identity financially, professionally, and even educationally.

Within these three broad categories if identity theft, the FTC associates seven types of fraud. These include credit card fraud, bank fraud, utility fraud, employment record fraud, government/benefits fraud, loan fraud and miscellaneous fraud.

How do fraud and identity theft relate? Where fraud is usually an isolated incident in which money is stolen or charged against an existing account, identity theft is more extensive. Identity theft involves the stealing of personal identifying information to initiate or transact business or make presentation in the name or person of another.

History

In the earlier part of the last decade, Prevent-Identity-Theft reported that that from the calendar year 2003 through 2005, the number of identity and fraud complaints increased from 542,656 to 686,683 representing an increase of 26.5%. Of this, the number of identity theft complaints rose 25.6% alone. Later research by this same organization disclosed that the incidents of cyber identity theft rose from 5,000 in the calendar year 2006 to approximately 35,000 at the end of the calendar year 2010. Today, it is estimated that there are 15 million victims of identity theft resulting in $50 billion in damages (www.identitytheftinfo/victims.aspx). This does not include cyber theft. According to the New York Times on November 14, 2012, the damages related specifically to cyber identity theft increase the estimated damages amount to $114 billion.

As researched by the National Conference of State Legislatures- Identity Theft 2012 Legislation (2012), to date, 34 states have introduced or have pending legislation regarding identity theft during the 2012 legislative session. The state of Alabama enacted three bills creating the Alabama Digital Crime Act, amending the definition of dealing in false identification documents and expanding the definition of identity theft to include using a person's identity to gain employment. The state of Colorado added a surcharge for individuals convicted of identity theft against at-risk adults or juveniles. The states of Kentucky and Michigan now allow exceptions to an insurer's use of credit information with regard to rates, rating classifications, tier placement and underwriting guidelines for specific life events, including identity theft. The state of Louisiana created the crime of online impersonation and enacted the Business Identity Theft Prevention Act. The state of North Carolina limited state agency identity theft reporting requirements. Utah lawmakers passed a bill requiring the Department of Workforces Services--if it learns during an eligibility check that an unauthorized person--to inform law enforcement and the Social Security number's owner, is using a Social Security number. And the state of Virginia enacted legislation that requires local departments of social services to conduct annual credit checks on foster children 16 years and older to uncover and resolve cases of identity theft or misuse of personal identifying information.

How does Identity Theft Happen?

Identity theft occurs in two primary ways which are classified as low tech methods and high tech methods. According to Stroup, a low tech method of identity theft refers to older means of stealing personal information such as by pick-pocketing or burglary. In current times, this list of low tech methods has expanded. Dumpster diving remains a very popular low tech method of identity theft. While most people think of bills or other forms of hardcopy with personal information displayed on it regarding dumpster diving, this form of identity theft also includes the stealing of discarded or donated computer equipment from which data is copied and manipulated for the thief's use. Phishing occurs when identity thieves present themselves as financial institutions and companies requesting personal information from a person either by telephone or electronically. Change of address also remains a popular low tech method. With this financial, billing, or benefits statements are redirected through submission of a change of address form or letter to the perpetrator. As well, stealing of personal information such as personnel records or business records continues to be employed as a means of identity theft; this type of theft is also popular with bribing. Pre-texting refers to presenting false pretenses to obtain personal information from financial institutions, telephone companies, health insurance companies, hospitals or other organizations as the thief poses as an employee from within the company or from another company to obtain personal information. Pre-texting may also occur as an identity thief poses as a person's representative or as themselves to a company in order to obtain personal information. Finally, shoulder surfing is a low tech method of identity theft commonly enlisted where the input of passwords or account numbers is observed and recorded as they are entered into computers, ATM's, or even registers.

High tech methods of identity theft include hacking, spoofing, skimming, phishing and cloning. Hacking involves the unauthorized accessing and manipulation of hardware and software. In simple terms, it is "breaking in" to a computer or network and retrieving information for personal use. On the other hand, spoofing occurs when attempts are made to make users believe they are receiving information or messages from a trusted source. It can also occur when websites are presented as secure. In both instances, users are requested to provide personal or financial information. Skimming involves a device that can be attached to an ATM machine, gas pumps, or any other form of

swipe technology. The skimming device copies the personal information from the swiped card into a data file on the device which is later retrieved by a thief and exported for the creation of credit cards, debit cards, ATM cards, or into a company's system in order to gain access to account information. As a high tech method, phishing establishes a website for a fake company which allows users to access information, subscribe, enroll or purchase by providing personal identification information. Similarly, cloning involves the recreation of a legitimate website of a licensed company where users capture personal information through transactions and input. While this website looks legitimate on the front end, captured data on the back end is again used for production of credit cards, accessing bank accounts or other personal files, or can even be used to collect funds by the imposter organization.

With high tech methods or as they are more formally known, data breaching, malware plays an important role in obtaining personal identifying information. Malware includes viruses, worms, and Trojan horses. Microsoft.com defines malware as unwanted software installed without consent. Viruses include software programs that that disrupt the operation of a computer. They come in various forms through texting, images, e-mail, audio and video files. The key feature of the virus is that they are programmed to be easily spread. According to North Carolina State University (n.d.), "worms are software programs that make copies of themselves" with the aim of compromising the security of a computer. Worms are programmed to enable copying of malicious software from one disk drive to another automatically, copying itself and generating an e-mail or other transport mechanisms to users. The Trojan Horse, conversely, does not replicate, but also compromises computer security. It does not automatically generate e-mails with malicious software embedded. Typically, Trojan Horses are intentionally sent from one user to another.

To gain understanding, consider the following example provided by Robertson (2012) in How Paper Bills Can Protect You from Cyber Theft. Robertson, utilizing the research of cyber security expert, Tom Kellerman, writes "They (cyber criminals) do this by initiating wire transfer requests the moment the victim logs into an online banking account. And, even spookier, they change the account balance and transaction history you see on your screen to hide the fraud. They use malicious code that kicks in after the user has logged into their bank's website." What happens is that a cloned screen of that victim's financial institution's on-line banking system is created. Each time they log on, transactions are written to this clone as well as to the account. The clone, however, keeps only the history and balance the victim expects to see. On the back end, though, the cyber theft has accessed their password and initiates wire-transfers to another account draining the actual account. This even goes to the extent of producing an on-line statement at the end of the period. Consequently, Robertson and Kellerman advocate receiving hardcopy bank statements as a safeguard.

Interestingly, this can be done by one person or by groups. Referred to as cyber theft rings, groups of thieves may work together specializing in malware encoding, exploiting and money mules. Encoders are software developers who write malicious programs which are sold on the black market to exploiters. Malware exploiters not only purchase the malware, but also launch attacks on bank accounts which allow them to transfer stolen funds and deter tracking of the activity. Money mules are the individuals responsible for the transfer of financial information and money and who keep a percentage for their services and return the rest to the exploiters. Their victims include children, teens, adults, deceased persons, businesses and financial institutions.

The target audience of identity theft, however, is four fold: the middle aged, teens and tweens, high incomers, and users of credit cards. According to McPherson (2012), the U.S. Department of Justice cites that people between the ages of 35 and 49 are the most at risk for identity theft with 2.76 million incidents reported for this group in 2010. This group is at risk because of their higher earning potential, greater number of credit cards in possession, and are perceived as less financially astute compared to other groups of adults. At the lower end of the age bracket, teens and tweens are prime targets, but not because they possess credit cards and bank accounts. With this target group, however, most cyber identity theft includes the opening of new accounts incorporating their personal identity information and a manipulated birth date in order to satisfy application requirements. High income earners comprised 2.83 million incidents in 2010 which is not surprising. Identity thieves perceive this group, who typically earns a minimum of $75,000.00 annually, as having more disposable income, and therefore are more attractive for the occasion of identity crime. Finally, according to the Department of Justice, credit card theft and fraud comprises 54% of all incidents.

No matter the class of victim or the type of identity theft committed, persons primarily discover they are casualties of an identity crime in three different ways: at hallmark points of life, through negative correspondence from a

business, or by companies who provide anti-theft services. Hallmark points of life include instances such as denial of job offers or promotions, at the time of a major purchase such as a home, or even application for a new or first credit card. Businesses may alert consumers of identity theft through denial of credit applications, collection notices, and receipt of bills for services not rendered by an individual, or notification by a government agency such as the I.R.S.

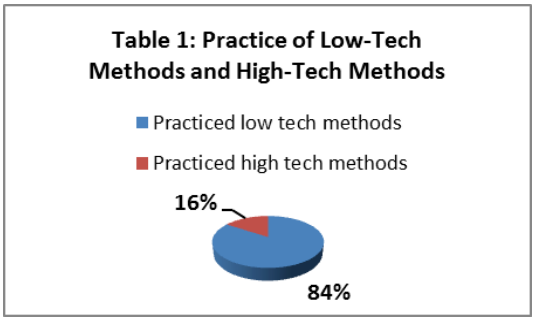
Measures to Avoid Identity Theft

Similar to the methods of committing identity theft, low and high tech models of identity theft prevention also exist. Low tech methods consist of shredding all mail including old and new banking statements, bills, credit card histories, loan offers, and tax reporting documents. They also include subscribing to paper banking statements to verify transactions especially if electronic banking is practiced. In addition, low tech methods of prevention also include locking confidential information in secured personal safes and not carrying originals of social security cards or passports. High tech methods range from simple computer interaction procedures to full blown technology prevention services. A low tech method regards password composition. Using long phrases and symbols makes accessing passwords more difficult for hackers. Another simple low tech method suggests establishing multiple web browsers or different computers to perform various tasks and functions which require the sharing or inputting personal identifying information. An additional procedural precaution against identity theft with technology concerns secure websites. As personal information is requested, users may verify the security integrity of a website through visual inspection as secure website addresses typically are formatted "https://" rather than "http://". Biomedical identification further provides protection against identity theft through the use of fingerprinting, speech patterns, retinal eye pattern, and facial structures recognition. Technology advances such as radio frequency identification chips and virtual credit cards attached to bank accounts are readily available and offer additional protection as well. Software enhancements such as pinpoint with cell phone technology allows for greater prevention of theft as the purchases made and location of the purchases are sent to the cell phone for verification by the owner. Finally, comparative analysis of anti-theft technologies like those offered through companies such as LifeLock and Identity Guard concludes that basic services such daily monitoring of fraud and credit bureau reporting for a fee are common to most services. While fraud monitoring concentrates on stopping the opening of new fraudulent accounts, credit monitoring is a service that attempts to control damages related to identity theft. Importantly, credit bureau reporting does not prevent the opening of new fraudulent accounts. These anti-theft technologies also promote additional Internet security at varying price point levels. Providing features like anti-spyware, anti-phishing software, anti-key logging monitoring, zone alarm benefits, firewall security, backup services, anti-spam software, anti-virus software, parental control software and file sharing network protection increase data security and the integrity of personal identity and can be obtained through these services for fee.

Research

After researching the legislation, history and statistics, and methods of identity theft and deterrence, a study was conducted at Blue Ridge Community and Technical College outside of Washington D.C. The research question was: What are the most commonly practiced forms of identity theft prevention, regarding low-tech and high-tech methods, employed by IT professionals also teach at the college level?

A quantitative methodology was enlisted for the study. The sample population consisted of full-time technology instructors and professionals who teach part-time and who are also employed in information technology (IT). Enlisting the information obtained through literature research synthesized above in this article, the goal of this study was to determine practices employed by IT professionals to deter theft of their personal and professional identifying information. Survey questions were formatted based on the suggested preventive procedures and technologies identified in the study of the literature.



To begin, it is important to note that two participants reported being a previous victim of some type of identity theft. Table 1, above, indicates the comparison between the low tech practices of identity theft prevention by participants and high tech practices. Of the 90 question responses received, 76 indicated regular practice of low tech methods represented by the darker portion of the pie chart. Conversely, as Table 1 illustrates, 14 indicated regular practice of some type of high technology method of prevention. Regarding low tech deterrence practices, approximately 67% of the participants indicated that they always shred documents disclosing personal data with an additional 33% indicating that is a usual practice. Of the participants, 45% of the IT instructors and professionals indicated that they keep confidential information in some form of locked safe or vault. Further, regarding low tech methods of identity crime deterrence, 78% of participants indicated that they always log off when leaving their computer while 66.7% reported employing multiple computers to conduct different transactions in which personal identification data is submitted. Interestingly, only three respondents indicated that they do not subscribe to this practice. From a final angle regarding low tech methods of identity theft deterrence, 56% of the IT instructors and professionals reported enlisting multiple web browsers as a means of identity theft prevention when completing functions requiring the sharing of personal identification information while all of the participants reported verifying the security of website as a regular personal practice of identity theft protection.

Conversely, the research showed that the employment of high tech methods of identity theft prevention was less frequent by IT instructors and professionals who participated in the study. Of the study participants, 22.2% indicated that they utilized anti-theft vendor technologies such as Life-Lock or Identity Guard as a means of on-line security and for fraud monitoring while almost 70% indicated that they did not employ similar technologies for credit bureau reporting services.

Concerning the enlistment of biomedical preventive technologies among the participants, the most popular technology was fingerprint recognition followed by facial structure recognition. None of the participants employed speech or retinal pattern recognition technologies as a means of identity security. Finally, regarding other technological developments aimed at limiting the occurrence of identity theft, none of the respondents employed pinpoint services with their cell phones; 11.1 % utilized v-card, and approximately 22% of the survey participants took advantage of RFID technologies in their personal strategies of identity theft prevention.

Given these results, this study reveals that low tech methods of identity theft are practiced more regularly by the IT instructors and professionals than the high tech methods presented and discussed. Logging off when leaving a computer and the shredding of hardcopy documents were the most consistent practices of the sample population. However, the responses regarding employing different browsers and computers when conducting transactions in which personal data is required suggests an additional safe guard utilized by this population with considerable frequency.

High tech methods of identity theft prevention such as subscription to companies which offer automated systems of fraud monitoring and credit bureau reporting were not frequently purchased by the IT instructors and professionals who were surveyed. More common were methods utilizing fingerprint and facial structure recognition software. Likewise, the use of v-cards and RFID technologies were indicated by these professionals as a preferred means of identity theft protection.

CONCLUSIONS

As presented identity theft has been on the rise since 2005. The number of incidents of cyber related identity theft is becoming more frequent also. The Federal Identity Theft and Assumption Deterrent Act of 1988 provided definition of identity theft acts, sentencing guidelines and established centralized complaint and consumer education bureaus in order to address this rising problem. While low tech methods of identity theft continue to be popularly employed, sophistication of technology driven crime such as those enlisted by cyber rings is becoming more complicated, thus making it more difficult to catch identity thieves. Complicated software, systems and operation rings have stamped their mark on approximately 15 million victims including the middle aged, teens and tweens, high income earners, and credit card users resulting in almost $114 billion in damages as previously presented.

Likewise to confront this increase in identity theft, low tech methods of prevention such as shredding hardcopy, utilizing safes and vaults, regular practice of logging off when leaving a computer, manually verifying the security of a website when personal identifying data is required in a transaction, and enlisting multiple computers and web browsers to perform functions requiring the input and access of personal data have proven to be highly employed as disclosed by the study conducted with IT instructors and professionals at Blue Ridge Community and Technical College. High tech methods such as fingerprint and facial recognition, RFID, and v-card technologies are becoming more prevalent means of identity theft prevention. Other fee based high tech methods such as fraud monitoring, credit bureau reporting, and expanded Internet security systems and services are adding additional preventive measures against cyber thieves for some users as the study of IT professionals conveyed. Whether you are a victim of identity theft or a subscriber to any of the prevention methods presented, however, there is an associated cost…and…the cost is all yours.

REFERENCES

1. Copes, H., Kerley, K.R., Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. Journal of Criminal Justice. Retrieved from: http://www.elsevier.com/copyright
2. Economist Intelligence Unit (2012). Cyber Theft of Corporate Intellectual Property : The Nature of the Threat. The Cyber Hub. Retrieved from: http://www.cyberhub.com/research/IP_threat/Index/17
3. Federal Trade Commission (1999), Prepared Statement of the FTC on Financial Identity Theft Before the Subcommittee on Telecommunications, Trade and Consumer Protection and the Subcommittee on Finance and Hazardous Materials of the Committee of Commerce, http://www.ftc.gov/os/1999/04/identitythefttestimony.htm, accessed September 21, 2003
4. Federal Trade Commission (2012). Identity Theft and Assumption Deterrence Act Retrieved from: http://www.ftc.gov/os/statutes/itada/itadact.htm
5. Identity Theft Resource Center (May 2008). Identity Theft: *The Aftermath* 2007. Retrieved from: www.idtheftcenter.org.
6. National Conference of State Legislatures (April 2012). Identity Theft 2012 Legislation. Retrieved from: http://www.ncsl.org
7. NextAdvisor (2013). Identity Theft Protection. Retrieved from:http://www.nextadvisor.com/identity_theft_protection_services/index.php?a=2&kw=gidtpb8+identity%20theft%20protection%20services+ntwk+g-fq-identity+theft+statistics&gclid=CJqP8dzB4bQCFQVgMgodmF8AGA&ref=www.google.com
8. McPherson, L. (2012). The 4 Groups Most At Risk of Becoming Identity Theft Targets. Retrieved from: Source: http://stumbleforward.com/2012/09/17/the-4-groups most-at-risk-of-becoming-identity-theft-targets/
9. Microsoft Safety & Security Center (2013). What is malware? Retrieved from:www.microsoft.com/security/resources
10. Murphy, N. (nd). An Insecure Future. Embedded Systems Programming. North Carolina State University. Retrieved from: http://ethics.csc.ncsu.edu/abuse/wvt/
11. Newman, G.R., & McNally, M.M. (2005). Identity Theft Literature Review. U.S. Department of Justice. Retrieved from: https://www.ncjrs.go

12. Robertson, J. (2012). How Paper Bills Could Protect You From Cyber Theft. TECH BLOG. Retrieved from: http://go.bloomberg.com/tech-blog/2012-12-17-howpaper-bills-could-protect-you-from-cyber-theft/
13. Sabadash, V. (2004). What is hacking? Computer Crime Research Center. Retrieved from: http://www.crime-research.org/news/05.05.2004/241/
14. Stroup, J. (2012). Identity Theft - How Identity Theft Happens. About.com Guide Retrieved from: http://idtheft.about.com/od/identitytheft101/a/HowItHappens_2.htm
15. Stroup, J. (2012). High Tech Identity Theft Protection. About.com Guide. Retrieved from: http://idtheft.about.com/od/preventionpractices/a/High-Tech-Identity-Theft-Protection.htm