Identity theft

Law, Crime

Identity theft is a growing problem and costs American consumers billions of dollars and countless hours each year. The following paper will discuss the issue of identity theft, the definition of the problem and it will survey five people about personal awareness of identity theft.

The largest transaction afamily, or individual will make is when they purchase a home. The first step in buying a home is to make sure that the family and/or the individual understand the risks of identity theft and how serious it can become. The Federal trade commission receives 15, 000 to 20, 000 consumer complaints every week. Identity theft can ruin a person's credit and derail that person's real estatedreams.

Related reading: Snatch Theft Essay

In fact, many consumers first learn they are victims of identity theft when they are in the process of renting or buying a home. This means that a person's or family's real estate dreams can be dashed in a moment because they were unknowingly a victim of identity theft. There are different avenues of choice a person can make in deterring identity theft and ensuring that one does not become a victim of such a crime.

Because the home buying process involves sharing a certain amount of personal information with third parties, home buyers should be careful when sharing financial or other personal information, whether in person, on the phone, or over the Internet. Many consumers are not aware that providing personal information online is in effect authorizing the owners of that site to sell the consumer's information to third parties. Therefore a person should only use trusted sites with security and/or privacy.

Recently NAR and the Federal Trade Commission formed a partnership to combat identity theft. The program, " Deter, Detect and Defend" aims to educate consumers, particularly homebuyers, about the devastating effects of identity theft and help them protect themselves against that crime.

In order to deter identity thieves, the FTC and NAR recommend that consumers shred financial documents and paperwork with personal information before discarding. This is because often times identity theft may occur when a criminal goes through a person's trash and finds credit card acceptance letters and thus, they get the card under the person's name all because the document was not discarded of properly or fully.

Another deterrent that a person may do in order to protect their identity is to protect their social security number. A person should only give out their social security number if absolutely necessary or ask to use another identifier. If a person on a phone asks for this number they could be writing it down to use for their own benefit; such situations could be billing statements and questions with a person's credit card company or any other billing service that wants a person to identify themselves with their social security number. An alternative to using one's own social security number is to use one's account number instead.

Another deterrent to identity theft is to not give out personal information on the phone by mail of the Internet unless the person knows with whom they speaking or dealing with. Many people with cell phones often times conduct business while they are shopping or while they are out in public. This is a very poor in judgment move to make because being in public and not aware

of one’s own surroundings is a vulnerable place to be conducting business. Many people forget in what surroundings they are speaking on their telephone and any eavesdropper can find out a person’s address, phone number, family members, etc.

Another item on a list of deterrents is to make sure no one in public sees a credit card. While standing in line at the checkout, camera phones have made it simpler and easier to be an identity thief; this is true because anyone who is behind someone in line using their credit card can simply take a picture of that card and have the account number for their personal use. Therefore it is behooving to be constantly aware of one’s surrounding, who is the next person in line and to make sure the account number of a credit card while in use remains private.

Thus, it becomes increasingly important to be able to detect suspicious behavior and activity everywhere. A consumer should then know a few things so that the previous situations do not occur. A consumer should routinely monitor financial accounts and billing statements. If unusual activity appears on a person’s account it should be reported to the credit card or billing company immediately so that if the consumer is a victim of identity theft the card will be reported as such and the next time the thief uses the card there will exist a paper trail by which the police can find them.

Another way in which a consumer can ensure their own protection is to be alert to signs that require immediate attention, such as bills that do not arrive as expected; unexpected credit cards or account statements; denials of credit for no apparent reason; and call or letters about purchases the

consumer did not make. Each of these items is a definite sign of identity theft. A smart consumer is cautious about these different signs and ensures of their own accord that such false accounts are not accomplished by shredding credit card offers in the mail, and by keeping proper and timely track of their own purchases.

Another way in which a consumer can safeguard against identity theft is to purchase monthly insurance from the credit card company that allows the consumer to be fully protected should identity theft occur. Such a program is set up so that when faulty account balances are detected the consumer does not have to pay for the charges.

If a consumer thinks that identity theft has occurred against them then they should place a ‘ fraud alert’ on their credit reports so that damages incurred during this period do not misrepresent the consumers own credit report since they were in fact victims of a crime and not actively ruining their own credit status.

A consumer who has been the victim of identity theft should quickly close accounts that have been tampered with or established fraudulently. This tells the credit companies that such accounts were initiated by the consumer since their action in repelling the accounts was swiftly taken.

Consumers should also file a police report immediately once they are certain that they have been exposed to identity theft. Filling such a report lets the police do their jobs in ensuring that such a crime does not persist and that the person or persons responsible for this crime are appropriately punished

and do not go back out into the business world thinking that they can easily repeat their actions without negative results. In order identity thieves to be put in jail the initial step is to file a police report.

Another action that a consumer can accomplish if they have been the victim of an identity theft is to file a report of the theft to the Federal Trade Commission. This further takesresponsibilityof the theft off of the shoulders of the consumer.

There of course ways in which identity fraud has been staunched by different companies. One way has been the introduction of virtual credit cards. This service is given by MBNA and is called ShopSafe. This service is found through MBNA's Net Access service for paying bills online. This means that a consumer can safely shop through their own browser or they can shop with a free down load desktop software. The virtual card has the option of the consumer choosing the duration of the card's active status, and the limit on the card as well. (Arar, 2006, 47).

Another option available for consumers is to pay by e-pay online. This option is available at different online merchants which dictates that the consumer pays electronically (this is typically used in billing statements). The site that has been utilized the most is PayPal. Everything on PayPal is done safely, and electronically. PayPal does not trade consumer information and does not allow the consumer's bank information to be directly seen by

The research done with PC World, 2006, initiates consumer awareness about how to appropriately use a computer that ensures personal account

information is not accessible by anyone else besides the consumer. In their section entitles Privacy Watch; How to Secure Files on Your Hard Drive, the article discusses how to files safeguarded. A consumer's computer should be appropriately safeguarded by using encryption software,

Files are encrypted only while on the hard drive. If you send an e-mail attachment to someone from your encrypted hard drive, the software automatically decrypts the attachment before it leaves the PC, and the recipient receives a normal unscrambled message. Full disk encryption tools used to have one major drawback: They slowed PCs considerably. But as processor power has gone up, software makers have optimized their products so effectively that you can barely tell the encryption is happening. I surfed the Web, checked and sent e-mail, and even played some graphically intensive games on the encrypted laptop without encountering a perceptible performance hit from the encryption software, which quietly went about its business in the background. 48.

The overall focus of PC World's article involved being a conscious consumer and careful shopper.

David M. Lynch's article Securing Against Insider Attacks (2006) also gives advice and warning signals of identity theft in regards to IT security. One such maxim listed is that of trusting the people who make up established relationships. This theory states that anyone within a person's ' tribe' is immediately trustworthy but an outside must be viewed with precaution, as Lynch states, " Since the very first IT survey on cyber attacks, one fact has remained almost constant: a greater percentage of attacks come form the

inside (from ‘ trusted’ folks)—60 to 70 percent—than from the outside (the ‘ untrusted’ folks).

Or, to put it another way, roughly twice the number of attacks come from the inside vs. the outside.” (40). This places a new perception on identity theft since the person who is the thieve is typically thought of as being a stranger, but in the above statement, Lynch points out that most of the time the person doing the thieving is someone the consumer personally knows.

Lynch goes on to state that identity theft has become such a staple crime is because of the broadening scope of business which has subsequently made the world a smaller place. Almost all business, large and small have processing orders all over the world This ensures that an electronic identity is abundant in the business world. This electronic identity when paired with repositories of personal information is the number one reason why identity theft has grown so widely (while the market grew in a global scale so did the crime of identity theft).

Lynch’s article highlights different banks and organizations that themselves have been victims of identity theft,

Data broker Acziom Corp. experienced identity theft by an insider that cost it $5. 8 million, including employees’ time and travel expenses, security audits, and encryption software…ChoicePoint said in February that thieves using stolen identities had created 50 dummy businesses that pulled data including names, addresses, and Social Security numbers on as many as 145, 000 people. As a result, its stock dropped from $48 a share the day

before the announcement to around $39. In May 2005, Wachovia corp. and Bank of America Corp. notified more than 100, 000 customers that their financial records had been stolen by bank employees and sold to collection agencies.

At the time of writing, investigators are still looking into the case, which may involve the unauthorized sale of data on nearly 700, 000 customers of various banks. In the same month, CardSystems Solutions Inc. confirmed it suffered a ‘ security incident’ in which an ‘ unauthorized individual’ infiltrated the computer network and may have stolen up to 40 million credit card numbers. 40

Each of these descriptions bears witness to the growing actions of identity theft not only toward consumers, or individuals, but also to large corporations and their customers.

Although identity theft is a growing concern it remains the act of federal laws but even more so of state laws that deter such a crime. New legislation has been put into place in different states such as North Dakota and California that ‘ forces companies to reveal unauthorized access to information that is commonly found in phone books’ (41). In California a more strict state law states that civil lawsuits to further deter identity thieves and punish existing thieves. There is also a law in effect for Arkansas, Georgia, Montana, North Dakota, and Washington that would require that state agencies and businesses inform residents if their Social Security numbers are disclosed (41).

Lynch describes the change of the face of identity theft and the laws enacted to prevent such a crime. The above paragraph mentions the initiative of states and governors to ensure that identity theft carries a harsh penalty but there is a contrasting point highlighted by Lynch that states that this state-by-state approach is very slow and seemingly impossible, "…for any organization that does business in multiple states to set up different levels of security and access on a stat-by state basis" (41). This means that companies will be forced quickly to set their own policies with the guidelines of the state in mind.

Lynch's article gives an example of a study done by the Secret Service National Threat Assessment Center (NTAC) and Carnegie Mellon University Computer Emergency Response Team (CERT) (published in May 2005) that gives details about insider attacks. This survey gave attention to people who had previously been exposed to internal access to information systems and used them fraudulently. The report however did not give a variable for the gain ofmoney.

The study was based on behavioral and technical viewpoints. These findings divulged that most of the identity thieves had previously been employees of the companies from which they stole (which goes back to Lynch's original idea of thinking people within the ' tribe' were trustworthy, while people outside of the tribe were not trustworthy), as Lynch states, " Most involved organizations identified financial losses, negative impacts to their business operations, and damage to their reputation as results of the attacks.

The impetus for most attacks was some form of negative work-related event, the most frequently reported motive was revenge, and the attacks were clearly a planned activity" (42-43). The identity thieves did not follow any profile but were simply employees or former employees of the company.

In regards to these attacks Lynch lists several ways in which a company or even a person can secure themselves from identity theft. The study conducted had employees without real technical experience gaining access to private folders and consumer identities. Lynch suggests that a layered defense that entails policies, procedures, and technical controls for protection. Lynch goes on to state that for IT there are specific procedures to follow to aid in preventing identity fraud which include, " Restrict remote access…Restrict system administrator…Collect information for all remote logins…Monitor failed remote logins…"(44-45).

The two main elements that a company of consumer should achieve in order to prevent such attacks include information gathering and analysis. Although the government on the federal and state level are making new legislations as to how to deal with identity fraud security on one's own computer is a good way to prevent the attempt of identity theft, as Lynch emphasizes, "…the first step toward this is understanding and acknowledging that we are all subject to the ' trusted tribe' mentality and that it is creating blind spots in our planning and implementation" (46). Thus, the ability to trust people, even those of the ' tribe' can be a misleading step in securing protection against identity fraud.

Surveys

Five people were surveyed for this research paper. They were asked qualitative questions with a few quantitative questions in order to provide statistics as to the percentage of consumers who had been victims of identity theft. The demographic for this research was based on male students ages 18-24 who either had or had not been victims of this crime. Their previous history with identity theft was given as well as their personal thoughts on how to counter identity theft. Here is a list of the questions the subjects were given to qualitatively answer: Have you ever been the victim of identity theft?

Do you know someone who has been a victim of identity theft? How were you or the person you knew victims of identity theft? Was the person who committed this crime against you someone you knew? What precautions do you take to ensure your identity is not stolen? Do you always take precautions of this kind? Do you think identity theft is a problem in the Unites States? Do you think identity theft is a problem on a global scale?

Of the five people given this survey three of them had been victims of identity theft. The ways in which the three people had been victims of identity theft all included stolen credit cards (or in one person's case, they had become a victim by someone else signing up for the credit card they had thrown away in a public trash can). In each of these three cases the victims were not in relation or did not know the person who stole their identity.

One of the other males surveyed had a relative who had been the victim of identity theft. His aunt had thrown away credit card acceptance letters and

her daughter signed up for the card and charged $5, 000 to the card within a month. The other male surveyed was not a victim of identity theft nor knew of anyone who had been a victim of such a crime.

Each respondent knew the ways in which they could secure their identity, especially the three who had already been victims, one of which states, " A lesson I only needed to learn once". Asked how they security methods for ensuring identity theft did occur they listed a tv commercial as to the main reason they knew how to handle their own trash and how to behave in public so that personal information was not divulged to strangers (each surveyed male listed the McGruff, Bite Out of Crime commercials as their main source of knowledge on identity theft and ways in which to prevent it).

The one surveyed male said that he always took precautions to ensure that his identity was not stolen; asked what these precautions were he said he owned a paper shredder and never took his garbage out at night but always during the morning right before the trash person was due to arrive. This surveyed male later told the researchers that he was studying to be a cop and so knew how to properly handle himself in the area of identity theft. The other males listed that they tore up credit card statements after receiving them. The surveyed male's aunt who had her daughter steal from her now throws her statements in the fire place (they live in the Northern Territory and so their fireplace is on most of the time).

The overall consensus to the question of identity theft being a problem in America all of the males surveyed answered positively. Asked whether or not they thought identity theft was a problem globally only two answered

yes (the male with the relative and the male who was studying to be a police officer). The rest of the answers for identity theft being a problem globally was answered negatively.

While there is no single answer to identity theft, the Federal Trade Commission, the police and also the credit card company itself may be allies to avoid this potential pitfall. A consumer has the responsibility to report fraudulent charges on their billing statement to ensure that other consumers' identities are not stolen by the same thief. A consumer must deter, detect and defend themselves against identity theft by all means stated in the above paper.

Bibliography

Arar, Yardena. (December 2006). Protect Yourself Against Credit Fraud. PC World.

Vol. 24, Issue 12. pp. 47-52

Lynch, David, M. (November 2006). Securing Against Insider Attacks. Information Systems Security. Vol. 15 Issue 5, p39-47.

Annotated Bibliography

Arar, Yardena. (December 2006). Protect Yourself Against Credit Fraud. PC World.

Vol. 24, Issue 12. pp. 47-52

This article focuses on different consumer actions that can be taken as a course of precaution against credit fraud. Such items as virtual credit cards and buying through PayPal were given as well as a detailed account of securing files on a computer through encryption.

Lynch, David, M. (November 2006). Securing Against Insider Attacks. Information Systems Security. Vol. 15 Issue 5, p39-47.

This article provide psychological background to the way in which consumers and companies perceive identity attacks which is dichotomized into the trust tribe, people within the company or in close relation to the consumer and the untrusted tribe, people outside of the company or strangers. The article also provided a brief study that highlights the demographic of identity thieves and the impetus for their actions.