Identity theft: A situation of worry

Passard C. Dean
Saint Leo University

Joshua Buck
Saint Leo University

Pierce Dean
Saint Leo University

ABSTRACT

Despite enormous advances in society and technology, millions of people have their identities stolen. Sensitive information is gathered through low-tech methods of physically acquiring it, as well as hi-tech methods that use various technologies to capture an individual's information. Yet, there are various tools and ways of preventing identity theft that is accessible to the everyday consumer, who either are ignorant of them or just cannot be bothered. This paper discusses ways that identity theft is carried out and ways to protect oneself. Additionally, a survey conducted by the authors revealed that many are not taking appropriate steps to protect themselves from this egregious crime.

Keywords: identity theft, SMSishing, phishing, skimmer, card swiping, identity theft prevention

WHAT IS IDENTITY THEFT?

Identity theft is described as "knowingly transfer[ring] or use[ing], 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" (Mercuri, 2006). That is, if someone takes another's personal information without consent and uses it in an illegal way, it is considered identity theft.

Identity theft is a prolific problem in today's environment. Millions of people every year are affected both directly and indirectly. There are numerous questions people generally ask when it comes to identity theft; however, there are three questions that encompass the majority of these questions. They are as follows: What is identity theft? How does identity theft occur? What can someone do to prevent identity theft? The goal is to answer these three queries to better equip the general populace in avoiding the adversity a person could face if he or she is a victim of identity theft.

In 2005, there were approximately 9 million people who were affected by identity theft. During that same period there was more than 200 million instances of data breaches. Additionally, there were more than 85 million instances of data breaches in the first quarter of 2008 (Prosch, 2009). In fact, the sheer volume of fraud in this area makes it one of the costliest crimes being committed.

The cost of identity theft can range from a small to an astronomical amount. No matter the amount stolen, there are other issues such as time and costs for recovery, which occur from identity theft. Many individuals and corporations are at risk for identity theft. On an individual basis, it can take as many as 175 hours for every incident of identity theft which transpires. This covers trying to make sure all the information from various companies is secure, changing any information that has been compromised, receiving reimbursement for the losses incurred, and adding protection to prevent identity theft from happening again. The out of pocket cost to take care of this amounts to approximately $1,500 per incident (Smith, 2005).

HOW DOES IDENTITY THEFT OCCUR?

Typically, a person who has their identity stolen will have their name, address, social security number, and even bank account number stolen. Certainly much more can be stolen, but those four pieces of information are particularly vital when a person is using someone else's information illegally. There are three main types of identity theft which are most prevalent in today's environment. The first and most prevalent is financial identity theft which is using someone's identity to purchase merchandise or establish a credit line (Norum, 2007). The second type is criminal identity theft. This is where a criminal will give law enforcement officer another person's information (Norum, 2007). Lastly, there is a type of identity theft called identity cloning. This form of identity theft involves a criminal taking every bit of someone's personal identity and using it to create a new life for themselves (Norum, 2007). Identity cloning is much easier when a criminal is stealing a child's information. The reason is that, more often than not, a child's history or identity will not be checked by the parents till they are at least 18 because there is generally no real reason to do so.

There are two common ways in which criminals may gain a victims information that will enable them to steal that individual's information. These are the "low-tech" and "hi-tech"

methods. Both methods have their advantages and disadvantages for criminals, and therefore must be investigated deeper to try and prevent the theft of one's identity.

The low-tech way of stealing a person's identity is just like it sounds. This method originated back in the pre-Internet era, but is still certainly a viable method of stealing one's identity today. In fact, this method works so well that in 2005, the Better Business Bureau did a study which concluded that traditional (low-tech) methods of stealing information was six times more likely to occur than hi-tech methods (Mercuri, 2006).

Some of the most common ways a thief might try to find information include searching through trash or mail, breaking into someone's house and stealing the information, and even breaking into a person's vehicle. Another method a thief might use is a technique called "shoulder surfing". This tactic is when a person looks over a person's shoulder and attempts to garner the information they are inputting (Haygood, 2006). An example of how a person might attempt to do this is at an ATM machine, where the potential victim who is inputting their pin number or account number could unintentionally disclose this information to the other person.

Another method used by identity thieves is attempting to get the victim to voluntarily disclose the information themselves. Many may believe this is not an effective method, but this technique is more effective than people would like to think. The technique itself is called "pretexting" which is using bits of a person's information in order to get them to reveal more information about themselves (Haygood, 2006). One way an identity thief might attempt to accomplish this is by calling a person, and making the phone call sound official to the victim. This could be done by the culprit telling the victim that it is their bank calling to verify information, which requires the victim to disclose sensitive information to the thief.

While the low-tech methods continue to be used, there has been an explosion in the use of hi-tech methods. There are numerous high-tech methods which thieves are now using so as to gather a person's information. Often, these methods require no interaction with the victim at any point during the information gathering or the crime stages.

The first type hi-tech method is the use of a device called a skimmer. A skimmer is "a high tech electronic device used to capture victims information when scanned" (Alberecht, 2011). This device is often installed onto a machine that a person would use to swipe their card. Often these machines are stand-alone ATM machines, or they are the card inserters at gas stations. These two are used often since there is little to no security watching over them, making them prime targets for the thieves to install the skimmers. The skimmers work the same way that any normal card swiping machine would work, which is to gather information. The difference between a normal card swiping machine and a skimmer is, instead of the information going to a bank, it is goes to the thief.

Another technique which thieves use is called "phishing". This method has become far more prevalent as thieves have become more technologically savvy in their methods. Phishing often stems from an official looking email. This email will often request the user to follow a link to a site in order to verify information. On the surface, both the link and the site look as if they are completely legitimate, but the issue is they are not. Sites are easily replicated if the source code is stolen, and only key links need to be changed to make it a fake website which a thief can use to steal information. The victim will believe it is a legitimate site, and this will lead them to typing in the information themselves, giving up any sensitive information a thief needs in order to steal the victim's identity. A variant of phishing is called "SMSishing". This is when a malefactor will send a seemingly authentic text from a bank saying to the victim that they need to update their banking information and to click the link just like phishing, or they could send a

text that appears to be from the potential victim's cellular provider to upgrade or to pay their account.

The final hi-tech method which will be discussed is the technique of hacking. Hacking involves a person or group of people working to infiltrate a person's computer, website or server in order to gain access to people's information. This method has become such a highly used way that in 2005 alone, 40 million people had their information stolen through hacking (Haygood, 2006). One of the issues with hacking is that it can compromise thousands, and even millions of people's information at one time. This was seen in 2011 when Sony had their network system compromised by hackers. These hacking compromised 77 million registered users, and the information stolen were names, addresses, and passwords to their Sony accounts (Baker & Finkle, 2011).

There is also another group which is identified by the name anonymous, but unidentified through the facelessness of the hacktivist group members. This group works together in an effort to hack or take down the person, business, or government entity which they disagree with. This group is responsible for taking down various sites temporarily and even hacking the servers to steal personal information. Often, the group will disclose entire documents on sites with malicious users who want to obtain the sensitive material. This allows any person who wants to attempt identity theft, have a shot at accomplishing this goal.

Recently, a man named Nate Anderson, who is a deputy editor at Ars Technica, tried a first-hand attempt at password cracking. The results he found are quite unsettling to say the least. With little to no experience cracking passwords, Nate was able to crack over 8,000 passwords by the end of the day through a little reading and help from the Internet (Anderson, 2013). If a person with no experience in the hacking and password cracking field is able to achieve cracking 8,000 passwords in a single day, then someone with plenty of experience is a real threat. With all of these threats, it might lead the regular person to question how they are supposed to protect themselves from having their identity stolen and falling victim to identity theft.

PREVENTING IDENTITY THEFT

There are many strategies a person may use in order to prevent identity theft. The most obvious method would be not to disclose the information. Often people are far too trusting if they receive a phone call that sounds official, and will disclose sensitive information to the person on the other side of the phone who may be a thief. An individual should never give out any information that could compromise their identity unless they are the ones who initiated the contact (Diller-Haas, 2004). Another method a person may use to facilitate the protection of their identity is checking their credit report at least annually or using an identity theft protection service such as LifeLock (Diller-Haas, 2004). While none of these services can guarantee 100% protection of individuals from identity theft, they represent an added level of security for the potential victim.

Another way of preventing identity theft is to destroy any documents such as mail which may contain personal information which a thief can use. It cannot be stressed enough that thieves will often rummage through a person's trash in order to find information about them which might have been kept on something as simple as a credit card application. The best way to avoid this from happening is shredding documents and throwing large amounts of the shredded documents out at once. Throwing a large amount of these shredded documents out at once will better mix the shredded pieces, which adds another level of security. Being able to stop the

chances of having a person's identity compromised because of mail can be prevented before the mail even arrives. There are millions of preapproved credit card applications that are sent out to people every day. All of these applications are easily accessible once they are put into the mailbox. A great way a consumer may avoid ever having it reach their mailbox is opting out of any marketing materials such as preapproved applications by calling 1-888-5-OPTOUT (1-888-567-8688) (Alberecht, 2011).

Another way to prevent identity theft is by the use of passwords. The use of passwords is an important way to protect access to information in today's environment. For passwords to be effective, it is imperative individuals create strong passwords. A combination of letters, numbers, punctuation, and special characters that hold a meaning to only the person who created the password is the best way to create one (Fordham, 2008).

Companies have just as much of a responsibility as individuals to protect a person's identity. To do this, more responsibility must be put on companies. Companies need to bolster their network security. Along with this, if there is a security breach, the company needs to notify any customers, users, or employees right away in order for the affected individuals to make the necessary changes to protect their accounts and information.

Additionally, the most important way a person can protect themselves is by paying attention. While an individual is never fully protected from having their identity stolen, paying attention to the details can help mitigate the issue. Often, people will become complacent with everything that is going on around them. As a result, they are less likely to notice something that might be out of the norm if they are not paying attention. Along with this, if a person is not using the tools they have available to them, such as access to their credit reports and checking bank statements carefully, then the person is leaving themselves vulnerable to identity theft.

IDENTITY THEFT SURVEY

To see how careful individuals are regarding their identity, the authors of this paper conducted a simple research. A questionnaire was created in Google Docs with a few brief questions. The questionnaire was made available to potential respondents through social media and email. There were 174 respondents. The results revealed that only 45 or approximately 26% of the 174 respondents check their credit reports on an annual basis. Additionally, only 27 or approximately 16% check their credit reports every six months. More disconcerting, 55 or approximately 32% of the respondents have never checked their credit reports. If the results of this survey are representative of the entire population, then it is no wonder identity thieves continue to flourish.

CONCLUSION

Identity theft is nothing to snicker about. With the many methods used by identity thieves to steal individuals' identities, the situation can seem very disheartening. However, doing a few, simple things can change it from daunting to doable. For instance, when sent an email from a contact you do not recognize, deleting it is a good idea. Also, when entering your pin into an ATM, make sure no one is around or can see your password. Doing easy things like this will likely save you the grief and struggle that comes from dealing with identity theft.

REFERENCES

Albrecht, C., Albrecht, C., & Tzafrir, S. (2011). How to protect and minimize consumer risk to identity theft. Journal Of Financial Crime, 18(4), 405-414. doi:10.1108/13590791111173722

Anderson, N. (2013, March 24). *How I became a password cracker*. Retrieved from http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/

Baker, L. B., & Finkle, J. (2011, April 26). *Reuters*. Retrieved from http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

Diller-Haas, A. (2004). Identity Theft: It Can Happen to You. *CPA Journal*, *74*(4), 42-44.

Fordham, D. R. (2008). How Strong Are Your Passwords?. *Strategic Finance*, *89*(11), 42-47.

Haygood, R., & Hensley, R. (2006). Preventing identity theft: New legal obligations for businesses. Employment Relations Today (Wiley), 33(3), 71-83. doi:10.1002/ert.20120

Mercuri, R. T. (2006). Scoping Identity Theft. *Communications Of The ACM*, *49*(5), 17-21.

Norum, P. S., & Weagley, R. O. (2007). College Students, Internet Use, and Protection from Online Identity Theft. *Journal Of Educational Technology Systems*, *35*(1), 45-59.

Prosch, M. (2009). Preventing Identity Theft Throughout the Data Life Cycle. *Journal Of Accountancy*, *207*(1), 58-62.

Smith, A., & Lias, A. (2005). Identity Theft and E-Fraud as Critical CRM Concerns. *International Journal Of Enterprise Information Systems*, *1*(2), 17-36.