Identity Theft: What You Don't Know Could Hurt You

Passard C. Dean

Pierce M. Dean

Jessica L. Dean

Saint Leo University
FL, USA.

Abstract

In this paper we discuss Identity Theft and various methods that are being used by identity thieves to purloin individuals' information. These include, but are not limited to, phishing, SMS ishing, skimming, juice jacking, and taking advantage of hotspots and public Wi-Fi. Also discussed are ways to mitigate your chances of experiencing identity theft. Therefore, you will be exposed to ways to better protect yourself against such attacks. Additionally, the authors conducted a simple survey on identity theft. Based on the responses, it appears the majority of individuals do not fall for the obvious emailing and texting scams used my identity thieves. However, there are some who do, which makes them vulnerable to the methods being used by identity thieves.

Keywords: Identity theft, Skimming, SMS ishing, Phishing, Juice Jacking, Wi-Fi

Introduction

No one is fully protected from identity theft, however, the more informed you are, the better able you are to protect yourself. Identity theft is the using of an individual's personal information without that person's consent. Based on information from www.identitytheft.info, it is estimated that "approximately 15 million United States residents have their identities used fraudulently each year with financial losses totaling upwards of $50 million."Additionally, this website also stated that "close to 100 million additional Americans have their personal identifying information placed at risk of identity theft each year."Identity theft has become such a problem in the United States that the IRS has created a cybercrime unit to fight this growing problem. While this unit is particularly directed at combating tax fraud, it goes to show the growing problem of identity theft (Cohn, 2015).

Methods of Identity Theft

There are various methods that are used by identity thieves. Some are very simple to execute while others require much more technical skills, hi tech equipment and software. We will discuss some of these methods, though we will not present an exhaustive list. In fact, identity thieves are constantly devising new ways to steal our identities.

Many individuals are not as vigilant with personal information as they need to, which allows identity thieves opportunities to steal their identity or, at a minimum, access their personal information and/or steal their assets. Simple ways in which an identity thief can access personal information is by searching through garbage cans or stealing mail from individuals' mailboxes. As such, it is imperative we shred all documents with personal information prior to disposing of them. Additionally, it is just as important not to leave mail in mailboxes overnight. Another simple method an identity thief may use is "shoulder surfing", which is a technique whereby an individual looks over a person's shoulder with the objective of attaining their information as he or she inputs it at an ATM machine or a supermarket checkout (Dean, Buck & Dean, 2014).This technique is very useful if the thief has already gotten the individual's card number.

Another simple method that is used by identity thieves is known as "pre texting". With this technique, the identity thief attempts to get information from the victim voluntarily. The technique is executed by the thief using bits of an individual's information in an attempt to get more information about the person targeted (Haygood, 2006).This is generally accomplished with a call to the targeted individual by the identity thief.

The thief attempts to convince the target to believe the call is an official call which needs immediate action and personal information. For example, the thief may pretend the call is from the individual's bank and that the information is needed or the person's bank account will be locked if verification does not take place immediately.

The techniques mentioned earlier or generally referred to as "low-tech" in nature. While they are still in use, identity thieves have gotten much more sophisticated, using "high-tech" methods. One such technique is called "skimming" in which a device known as a skimmer is used. A skimmer is "a high tech electronic device used to capture victims information when scanned" (Alberecht, 2011). Skimmers are generally installed on card reader devices where individuals swipe their cards such as at an ATM machine or gas station card reader. The skimmer can be place on the outside or on the inside of the machine. Skimmers look and work similarly to any card reading machines. The problem is that after the individual swipes the card the information is transferred to the identity thief, not the financial institution that issued the card.

Another technique which thieves use is called "phishing." This method has become far more prevalent as thieves have become more technologically savvy in appropriating individuals' information. Phishing often stems from an official looking email. The email generally requests the targeted individuals to click on a link that will take them to a site in order to verify information. While both the website and link look legitimate, they actually are not.
This is why it is imperative individuals refrain from providing any sensitive personal information on websites based on email requests. Reputable organizations will not request personal information in this manner. Another technique similar to phishing is known as "SMSishing". This method involves the identity thief sending a text message that appears to be coming from a financial institution to the targeted individuals, requesting them to update their banking information by clicking on a link. It could also take the form of a text requesting the individuals to pay the amount due on an outstanding account.

Juice jacking is one of the more recent "hi tech" methods of stealing an individual's information for malicious reasons. So, what is "juice jacking?"According to the website TechAdvisory.org 2014, juice jacking is achieved "during the charging process whereby user access is gained on your phone by leveraging the USB data/power cable to illegitimately access your phone's data and/or inject malicious code onto the device."The website goes on to say, "the attach can be as simple as an invasion of privacy, wherein your phone pairs with a computer concealed within the charging kiosk and information such as private photos and contact information are transferred to a malicious device."While that may seem bad enough, it could be much worse. The perpetrators can arrange for "an injection of malicious code directly into your phone."Security researchers believe a phone plugged into one of these charging stations could be infected within one minute of being plugged in (TechAdvisory.org, 2014).Furthermore, the website continues on to say that after being plugged into one of these "infected" kiosks, there could be lingering problems even if malicious code was not immediately injected."Once a device is paired to a computer, the code can access a host of personal information on said device, including your address book, notes, photos, music, sms database, typing cache, and even initiate a full backup of your phone, all of which can be accessed wirelessly at any time." (TechAdvisory.org, 2014).If this sounds scary, it is! These kiosks are generally located in high traffic areas such as, airports, amusement parks, coffee shops, and bookstores.

So how do you avoid being juice jacked? According to TechAdvisory.org 2014, the most effective precaution is not to charge your phones at these kiosks. Additionally, the website provides some simple tips on avoiding using public kiosk chargers as follows:

- Keep your devices topped off (fully charged)
- Carry a personal charger
- Carry a backup battery
- Lock your phone
- Power the phone down
- Use power only USB cables

The final "hi tech" method of identity theft addressed in this article is the utilization of public Wi-Fi. Larry Higgs2013, in a USA Today article stated, "Public Wi-Fi is inherently unsecure."He goes on to report that, "Anyone using it ought to do so with the premise that everything you do is visible to a third-party stranger with access to that hot spot."This statement was made by Kevin Clark, a cybercrime expert. While you can locate a public Wi-Fi almost anywhere, it is imperative you resist the temptation of performing any financial transactions or any other activities including your passwords on them.

You want to be especially vigilant by not utilizing your credit cards on these hot spots. In addition to the fact that your information is available to strangers, another significant problem with an open Wi-Fi is that you may believe you are on a legitimate Wi-Fi when in actuality you have connected to a "rogue access point" created by someone with malicious intent.

Survey

Methodology

In an attempt to ascertain how careful individuals are with providing important personal information to others, we conducted a simple survey. In addition to gathering some basic demographic information, the survey was used to elicit responses to the following questions.

1. How often do you check your credit report?
2. When typing in your pin, are you careful that no one sees it?
3. How do you dispose of documents with personal information?
4. How do you handle emails requesting usernames, passwords, credit card details, and/or money?
5. How do you respond to text messages requiring you to call a specific number or visit a certain website?

The questionnaire used to conduct the survey was created in Google Docs. It was then disseminated to respondents through the mediums of email and social media.

Findings

A total of 174 individuals responded to the questionnaire. Of the respondents, 117 were females while 57 were males. Of the total respondents, 15.5% checked their credit reports semi-annually, 25.9% checked their credit reports annually, 27.0% rarely checked their credit reports, and 31.6% have never checked their credit reports. Of the females, 43.6% check their credit reports either annually or semi-annually, while 36.8% of the males check their credit reports either annually of semi-annually.

In response to the question of disposal of documents with personal information, 88.5% either cut up or shredded them while 11.5% throw them away. Of the females, 91.5% cut up or shredded the documents while 82.5% of the males did the same.

Regarding the question about securing pin when typing it, 90.8% of the overall respondents say they are careful that no one sees what they are typing. Of the females, 91.5% are very careful about securing their pin while 89.5% of the males do the same.

In responding to the question regarding emails requesting usernames, passwords, credit card details, and/or money, 82.8% delete them, 15.5% open then delete them, and 1.7% provided the requested information. Of the females, 84.6% delete the emails, 14.5% open then delete them, and 0.9% provides the requested information. Regarding the males, 78.9% delete the email, 17.5% open then delete the email, and 3.6% provide the information. Regarding requests through text messages to call a specific number or visit a certain website, 98.3% delete the text message immediately, while 1.7% followed the instructions.

Conclusion and Advice

Identity theft is a rapidly growing offense in the United States. From 2012 to 2014, identity theft crimes grew by almost 7% which may not sound large; however, when looking at the actual figures of 16.5 million cases in 2012 to 17.6 million cases in 2014, it can be quite alarming (Programs, 2015). As our society advances with new technology, so do our criminals with their methods of thievery. Many of us do not think how much of our information is on the internet and can be accessed easily by our lackadaisical attempts at being secure. Based on the survey conducted, it appears the majority of individuals do not fall for the obvious emailing and texting scams, however, there are some who do, which makes them vulnerable to identity thieves.

While there are simple techniques we can use to protect ourselves, there are organizations we can utilize to assist us in this area of our lives. These organizations provide credit monitoring services at affordable costs. While we do not recommend any in particular, we believe it is a very good idea to get one of these organizations help protect you from new account fraud. Though the credit monitoring services cannot stop the fraud from happening, they are able to inform you of the fraud much earlier than you would have known about it. Some will also assist you in taking care of the negative impacts of the fraud.

If you are unable to pay for credit monitoring services, a low-cost alternative is something known as a "security freeze."If you execute a security freeze, this will lock your credit files at Equifax, Experian and TransUnion, the three credit reporting bureaus. This lock will remain in effect till you choose to unlock your files. Implementing a freeze has the effect of stopping new accounts from being opened by identity thieves. This is the case because potential creditors are barred from checking both your credit score and credit report. If you chose to apply for credit, you can use your password or pin to stop the freeze.

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.

Dean, P., Buck, J., & Dean, P. (2014). Identity Theft: A Situation of Worry. Journal of Academic and Business Ethics.

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

http://www.identitytheft.info/victims.aspx - retrieved on May 12, 2015

http://www.accountingtoday.com/news/tax-practice/irs-creates-cybercrime-unit-to-battle-identity-theft-74575-1.html- retrieved May 11, 2015

http://www.usatoday.com/story/tech/2013/07/01/free-wi-fi-risks/2480167/- retrieved on April 26, 2015

http://www.techadvisory.org/2014/09/whats-juice-jacking/ - retrieved on September 27, 2015

Programs, O. o. (2015, October 5). *Bureau of Justice Statisics*. Retrieved October 6, 2015, from Identity Theft: http://www.bjs.gov/index.cfm?ty=tp&tid=42