Fall 2010

Preventing Computer Identity theft

Donald R. McDaniel
Regis University

PREVENTING COMPUTER IDENTITY THEFT

SUBMITTED ON 11 OF DECEMBER, 2010

TO THE DEPARTMENT OF COMPUTER SCIENCE

OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES

OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN

INFORMATION ASSURANCE

BY

Donald McDaniel

Donald R. McDaniel

APPROVALS

Paul Vieira, Thesis Advisor

James A Lupo

James A. Lupo

D. M. Likarish

Daniel M. Likarish

Abstract

The arrival of the information age has created new challenges to the ability of individuals to protect the security and privacy of their personal information. One such challenge is that of identity theft, which has caused a number of hardships upon its victims. Perpetrators of this fraud may use identities of others to obtain loans, steal money, and violate the law. This paper will discuss the characteristics of the offenders and victims of identity theft. A systematic approach for preventing identity theft will also be presented with the hopes of curtailing this epidemic.

Acknowledgements

The author would like to thank his family, for their love and support throughout his entire life and more in particular during the past two years. Finally, he would like to thank his friends and colleagues from work for their encouragement to complete this degree.

Table of Contents

Page

List of Figures

Page

List of Tables

Chapter 1 - Introduction

Consider this as a possible scenario: An individual with a stainless credit history decides to purchase a new vehicle at a local car dealership. With the intent to finance the vehicle with credit that has been arranged by the dealer, they will complete a standard credit application. After the salesman conducts a credit history check, the individual may be upset to hear that their credit application has been denied. After a further investigation, the individual may find out the credit reporting agency lists twenty open lines of revolving credit and two different car loans. The individual may also discover that it lists 5 different residences over the past year. Even though there has never been a delinquent payment, almost every one of their creditors has reported the individual in default. In addition, these credit lines were never opened by this individual. It is apparent that a perpetrator stole the individual's identity and used their flawless credit to obtain thousands of dollars' worth of goods and services. After the credit limit has been exhausted, the perpetrator moved on to their next victim, leaving the individual's credit ruined.

The comment, "Information is power," is even more accurate now in the age of the computer and Internet. Information about us has been gathered from the time that we were born up until the day we die. Numerous files about us continue to live in computer databases for years, long after we leave this plane of existence. In a variety of situations, information can provide a critical edge. For example, personal information databases may be used to manipulate consumer behavior or sway public opinions for or against a specific policy.

Identity theft continues to be one of the fastest growing crimes of the new millennium across the globe. A perpetrator may steal the single most important asset anyone has: a sense of self – identity. Our identity is what defines one from the next person. Our identity provides a singularity in the world, which also allows the world to know that it is dealing with one individual out of billions of other people.

In order to determine an individual's identity, certain nonnumeric and numerical characteristics of each individual should be utilized. "Ideally, these characteristics should not change, and when we single out enough of these qualities, we should be able to identify each individual." (Newman, p. 1) One distinct physical trait most people are aware of is fingerprints. The likelihood of two people having identical fingerprints is so remote that it is statistically minute. This will serve as a primary tool for police agencies when identifying criminal suspects.

Qualities that seem to remain static are generally categorized as base identifiers. Base identifiers would be such items as the following: sex, race, birthplace, birthdate, and eye color. Most identification documents such as passports and drivers licenses use a combination of these attributes in addition to the individual's full name to create a unique identity for each person. The chances of two people sharing the same full name, birthdate, sex, and race is relatively slim. In the United States, the most important base identifier is the Social Security number, because it remains with the individual over the course of their lifetime. The Social Security number has become a wanted item of information for all sorts of reasons. In theory, every Social Security number should have information associated to only one unique person. This is why credit bureaus, universities, military, banks, and other agencies require the number.

The nation's insurance companies and credit bureaus have heavily relied on Social Security numbers. In essence this can be used as a file retrieving tool. The growth of the Social Security number as a genuinely national identity number virtually means that records associated with this number are considered to be very private. An individual's life history can be retrieved just with this number.

Identity thieves are preying off of this fact all too well. They are also aware that government and the private sector are computerizing private records which allow one agency or business to cross reference records that may be stored elsewhere. In a matter of minutes, an identity thief can put together a laundry list of information on nearly any individual in America. An individual being victimized by identity theft can be very severe. Victims of identity theft may have their credit ruined; others may be suffering from more dire consequences. Some victims have been arrested for crimes they did not commit. By having criminal records created in their name, or being made the subject of a lawsuit because a perpetrator has been using their identity. We are all exposed to becoming victims of identity theft, but I will discuss security measures that may be utilized to help mitigate these risks.

Chapter 2 – Review of Literature and Research

Chapter 2.1 – What is Identity Theft?

Although, there is no commonly accepted definition of identity theft, it may prove to be impossible to study the real threat of this anomaly without conceptual clarity. “Identity theft is the appropriation of an individual’s personal information to impersonate that person in a legal sense.” (Vacca, p.4) Identity theft is not a new concept. It has been around for a long time. At one point in time an individual could escape their life and disappear to a faraway land, pretending to be someone else. The consequences of stealing another individual’s identity did not have the far reaching impact that exists today. These were the days before the high tech methods of credit reporting and sharing information was commonplace.

Identity theft can still be done by low tech tactics as previously described above. However, identities can also be stolen using highly technical and elaborate means of obtaining the personal information of a stranger. Identity thieves that use the highly technical means are able to assume someone else’s identity very easily. The individual’s reputation can be devastated by the loss of their good name and the personal or financial mess that results. Thieves could be relatives, roommates, estranged spouses, friends, or colleagues from work. All of these people in some capacity may have access to their victim’s personal information.

2.2 - How Identity Theft Is Done

Identity theft is considered to be a “white-collar” crime and continues to emerge as a problem of the twenty first century. It is considered to be a faceless crime which means the perpetrator feels guilt free not knowing who the victims are. This skilled person will take the time to do research on their victims, learn new techniques, and finally execute the planned attack. While the perception may be that there are technical savvy criminals in far off countries using sophisticated means to steal identities, as mentioned earlier most identity theft cases involved low tech methods and involved someone the victim knows. Although, there are organized identity theft rings around the world, the likelihood of one's identity being stolen by a family member is far greater.

"It should be noted that identity theft in its many forms is a growing problem and is manifested in many ways, including large scale intrusions into third party credit card processors, theft from the mails of printed checks, pre-approved credit card offers and mortgage documents, credit card skimming, phishing schemes, and telephone and bank frauds, much of which is perpetrated through the use of SPAM e-mail." (Gerdes, p.25) The following are some of the ways that perpetrators may acquire and use your personal information and assume your identity:

- Dumpster Diving – Perpetrators rummage through trash, both of individuals and businesses, looking for personal information or bills.
- Skimming – Perpetrators obtain debit and credit card numbers by using special storage devices while processing the individual's card.
- Phishing – Perpetrators pretend to be a financial institution or another company that sends out popup messages or spam to get an individual to disclose their personal information.
- "Old-Fashioned" Stealing – Perpetrators steal purses and wallets; mail, including credit card and bank statements; preapproved credit offers; tax information or new checks. Perpetrators may also steal personal records from their employers or bribe employees who may have access.
- Changing Your Address – Perpetrators may divert an individual's billing statement to another location by completing a change of address form.
- Internet – Perpetrators can use the Internet to hunt down victims very easily. Genealogical databases give perpetrators access to maiden names, which are often used as passwords to bank accounts.
- Pretexting – Individual's may be duped into giving out personal information over the phone with a perpetrator who has disguised themselves as a representative of a reliable company.
- Onlookers – Individual's may expose their ATM card to a perpetrator that is looking in a public place. Perpetrators may use binoculars, camcorders, or a zooming camera.

2.3 - How Personal Information Can Be Used Against You

> Armed with a person's identifying information, an identity thief can open new accounts in the name of a victim, borrow funds in the victim's name, or take over and withdraw funds from existing accounts of the victim, such as their checking account or their home equity line of credit. (Gerdes, p.22)

Once the perpetrator has basic information about the individual, there are a number of ways it can be used. For example, if the perpetrator has seen the individual's credit card, they now have information on who may have issued the credit card. They now can call the financial institution and request a change of mailing address. Once the perpetrator has the card, they now can run up charges on the individual's account. The individual will never realize what is happening because they have never received a bill. By the time the individual wonders what has happened to their bill and contact the credit card company, it is too late.

A perpetrator that has access to an individual's personal information can take out the following loans in your name: car loans, house loans, boat loans, and so on. If the perpetrator is good enough, they will have all of the goods and the victim is stuck with the bill. If a perpetrator is able to obtain new checks or steal your checkbook through some illegal scheme, they will have the ability to bleed the bank account dry before the victim has any knowledge on what has occurred. In other words, a perpetrator can hurt the unsuspecting individual by opening a bank account in the victim's name, possibly take out cash advances from the victim's bogus credit card, and write bad checks against the account as often as possible before the bank reports the villainous conduct.

In the most extreme cases, a perpetrator may file for bankruptcy under a victim's name. This would prevent the identity thief from having to pay debts incurred under the victim's name.

Possibly, a perpetrator that is living in an apartment or house may file for bankruptcy to avoid eviction. A perpetrator could always file for bankruptcy, if they have a personal vendetta to cause an individual harm, this would be the perfect way to punish the victim.

The possible scenarios described are some of the ways that the theft of a victim's identity can cause havoc in their everyday life. Just thinking about this should be enough to scare the day lights out of us. This should definitely serve as a wakeup call to be more proactive to protect oneself from identity theft. Currently, sloppy credit granting procedures allow identity thieves to take advantage of these opportunities. Many credit card companies are not doing their due diligence to verify records. These companies are more interested in capturing new applicants than taking the time to confirm their level of authenticity.

2.4 - Techniques of Online Identity Theft

"But it is a relatively new marketplace, and trust takes time to build up, particularly when transactions take place across borders and recourse in the event of fraud is unclear." (Stein, p.67) As the number of online identity theft continues to rise, online retailers and banks have struggled to stay on top of the problem and to protect their clients, whose online account details and personal financial information are coveted by identity thieves. This makes online identity theft especially brutal on its victims, and makes the online community that bit more skeptical. Continuing to build online confidence remains a key challenge not just for the future growth of the Internet economy, but for assisting in the battle against identity theft. The challenge for building confidence is that the perpetrators techniques continue to evolve.

2.4.1 - Phishing

"Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients." (2009) Just like a lure might be dangled in front of a fish to deceive it into thinking there is a real worm at the end of the hook, phishing is instant messages or e-mail that look like they're coming from a legitimate company to get individuals to click a link so that they may provide their personal or account information. The term phishing first appeared in 1996 when perpetrators stole account information from America Online (AOL) using email as the fishing hook to steal passwords from AOL users. Phishing is a hybrid technique in the sense that it involves both the use of social engineering and technological means by disguising itself as a trustworthy company in an e-mail message. These scams may falsely claim to be from banks, brokerage firms, Internet auctions sites, credit card companies, electronic payment services, or some other service that consumers use. To appear authentic, these emails may use the following:

- The names of real people.
- Genuine looking graphics and logos.
- Links to pages of a legitimate website.
- Credible looking email addresses, such as "support@[name of financial organization].com".
- Formal looking references to laws.

Phishing messages have become extremely complicated, such that consumers cannot easily discern them from legitimate messages from the targeted organization. Most emails attempt to lure consumers into providing their personal information by requesting that they provide it in a reply email or by clicking on a link to a website that imitates a legitimate organizational website and asks them to provide information. Once the perpetrator has access to the victim's existing accounts, they can now withdraw money or purchase expensive merchandise or services. Phishers can also use the information to open new credit card or bank accounts in the victim's name. These various tactics may be used to lower the guard of consumers:

- Your account may be shut down unless you update your information.
- Please verify your identity because your account appears to be used by a third party which is a violation of the law.

- Due to a technical update, you will need to reactivate your account.
- Recent adjustments in the law require users to identify themselves.
- Security measures have been implemented to protect your account from identity theft requiring you to verify your account information.

Phishing messages may at times direct consumers to a fake website, or to send in the information by phone or fax. Viruses and worms can also spread the phishing email further, via victims' address books. These sites also count on the familiarity by the average consumer of details which differentiates legitimate websites from unlawful imitations. Domain names of spoofed sites often use small variations of the real site's domain name, such as www.beestbuy.com instead of www.bestbuy.com.

"Phishing attacks in the United States soared in 2007 as $3.2 billion was lost to these attacks, according to a survey by Gartner, Inc." (McCall, 2007) Most phishing attacks are directed at U.S. consumers. Symantec conducted its own survey during the year of 2009 and it found 1 in 352.2 emails compared to 1 in 244.9 in 2008 were phishing attacks. It was found that more than 161 billion phishing attacks were in circulation. Gartner research produced a report in 2009 and it found that in 2008, 80% of the adult population had received emails that appeared to be part of a phishing attack. This report also found that millions of users fell for the same scam every year. It should be noted that some phishing emails and websites look so authentic they have the potential to fool even the most cautious internet users. The top ten exploited websites are the following: Visa, HSBC, Amazon, United Services Automobile Association, Bank of America, Internal Revenue Service, PayPal, and Bendigo Bank (Australia).

2.4.2 - Pharming

"Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent." (2007) Pharming can also be known as domain spoofing. It is the use of a spoofed website persuading unsuspecting victims into releasing their personal information to the identity thieves. This technique is much more difficult to prevent and it may affect a high volume of users per attack due to multiple website visits.

There are two different techniques on how pharming can be accomplished. The first involves the use of a Trojan or virus to change the victim's host file. This text file is left over from the earlier days of the Internet, and is used to connect a web address to a specific machine IP address. This pharming method changes this file to connect the web addresses of well-known financial institutions and banks with the IP addresses of phishing sites, so when the users open their browsers and enter the web address of their bank, they will be redirected to the phishing site instead.

The second pharming technique is equally menacing and it is known as Domain Name System (DNS) poisoning. DNS replaced the local host file as the process for resolving a web address to a particular IP address. Vulnerabilities in DNS software are manipulated in order to gain control over the domain name of an existing website. The numeric IP address that is related to the domain name is then modified. The end result is that a trusting user enters the website address that has been changed in their browser, and they will automatically be taken to the spoofed website. The victim's browser may display the correct web address, but the site being viewed will be a sham. By the time the user unknowingly logs onto the fake website with their username and password credentials, the perpetrator has already hijacked the victim's information. "Identity thieves are able to deceive everyone who attempts to log onto a compromised website, making detection extremely difficult while permitting access to mass amounts of personal information." (Perrl, p.4)

2.4.3 - Spyware

Spyware is one type of malicious software (malware) that gathers information from a computer system without the users consent. Spyware has been known to cause computer slowdowns or system crashes as well as unwanted advertising and continuous popup messages. However, the more serious consequence includes identity theft. Spyware has the capability to monitor nearly any activity of data that is related to the users computing environment. Not only are the files that reside on a hard drive is tracked, but spyware can also include volatile data such as keystrokes, screen shots, and data packets observed on connected networks. Users may experience the following characteristics if spyware has been installed:

- Computer may run slower or crash more often.
- A new toolbar appears in the user's browser that may have not been wanted.
- The browsers default start page or search settings change without warning.
- Multiple popups appear even though a user may not be connected to the web.

Some spyware can also be used on cell phones, PDA's, and smart phones. These software applications enable perpetrators to mine through banking information, PIN codes, credit card numbers and other financial information, and all of this can be done remotely. Once the perpetrators has the information, they may elect to either sell it to others or use it for themselves for spam, marketing, financial crimes, or identity theft.

Another new phenomenon is called cell phone snooping. "Cell phones are loaded with so much personal information – and have so many new capabilities – that phone hacking has been the holy-grail for computer criminals for some time." (Sullivan, 2007) By installing spyware on a cellphone, a perpetrator will have the ability to watch and listen to the targeted victim in the bathroom, bedroom, or office meeting, by utilizing the devices microphone and camera. Perpetrators will have access to the most intimate details of the victim's life by recording private discussions between friends and family and snapping pictures of what they are wearing.

2.4.4 - Viruses

"A computer virus is a program that secretly attaches itself to another document or program and executes when that document or program is opened." (Ciampa, p.48) These programs have the intention of being malicious that can range from changing or deleting files, making a computer behave strangely (displaying messages), or wiping the contents of the user's hard drive. Once a virus has been executed it is designed to replicate itself to another computer to attack. Presently, viruses primarily spread through email attachments. After an infected attachment or program on the user's computer has been executed, the user may experience the following characteristics that they have a virus on their computer:

- Computer may restart on its own and fails to run in a timely fashion than the user may be accustomed to.
- Applications may not work properly.
- Computer may crash and restart every few minutes.
- Drives may be inaccessible.
- Computer consistently locks up often.
- Computer will gradually run slower than normal.

Some of the most troubling viruses are those that have been programmed to gather private information. This can include email passwords, banking information, and other data that may lead to identity theft. Last year a new type of banking virus was discovered that just did not steal user bank log in credentials, but will also steal money from your account while the user is logged in and viewing a fake balance. This virus is known as the URLzone and it is controlled by servers in the Ukraine. This virus is designed to steal money from user accounts based on how much money is actually in the account live in realtime while the user is logged in.

2.4.5 - Keylogger

"A keylogger is a hardware device or a software program that records the real time activity of a computer user including the keyboard keys they press." (Mitchell, 2010) Normally, keyloggers are used in IT organizations to troubleshoot technical issues with computers and organizational networks. Businesses or family members will also monitor the network usage of users without their direct knowledge. Lastly, identity thieves will use keyloggers on public computers to steal credit card information or passwords.

A keylogging program does not always require physical access to the user's computer. This can be purposely downloaded by a perpetrator who wants to monitor the activity of a user. Keylogging may be downloaded unintentionally as spyware and executed as a remote administration Trojan horse.

> A keylogger program typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file (which does all the recording) and an executable file (.EXE) that installs the DLL file and triggers the work. (2009)

Normal keylogging programs store the user's information on the local hard drive, but some are programmed to automatically broadcast data over the network to a remote computer.

2.4.6 - War Driving

Today, wireless networking continues to be one of the most popular and fastest growing technologies on the market. From home to organizational wireless networks, users are eager to take advantage of the convenience and freedom that this technology promises. Even though wireless networks are convenient, it is not always deployed securely. Improperly configured wireless networks are found in user's homes and in large organizations.

"War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere." (2002) This form of identity theft, perpetrators take advantage of wireless technologies, which allow families to have several computers connected to the same network. War drivers drive through neighborhoods, seeking out wireless networks. PDA's and wireless equipped laptops coupled with software that is available on the internet are used to find unsecure networks.

In the event an unsecured network has been detected, the perpetrator can use it to access the user's computer. Once the thief has infiltrated the user's computer, they may be able to obtain passwords and other personal information, such as credit and bank information, from files that have been stored in the computers that are available on the network. In 1984, the first publication about unsecured wireless networks is circulated in a magazine called "2600". This magazine contains information on codes and passwords about vulnerable areas for stealing network bandwidth.

2.5 - Mitigation of Online Identity Theft

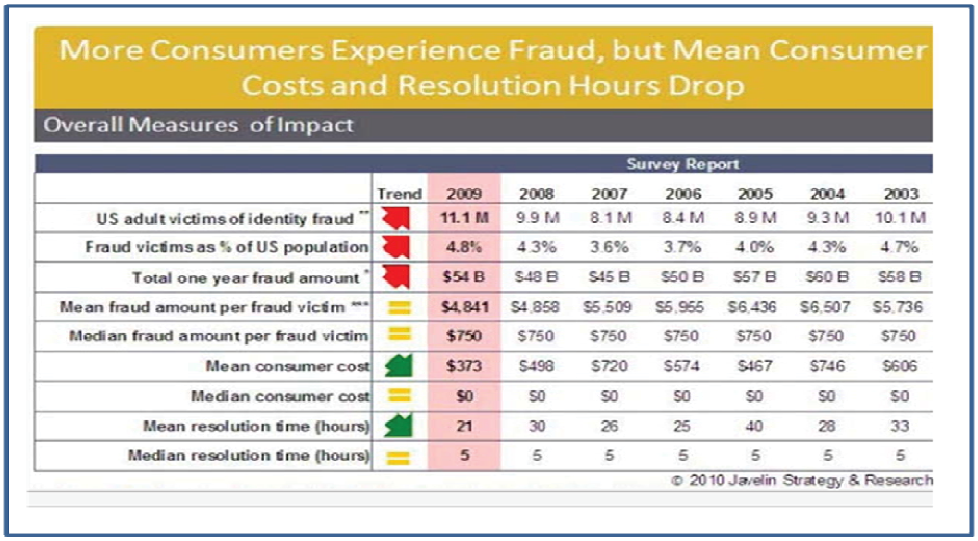
"Many victims thought better awareness on their own part of how to prevent and respond to identity theft would have been most helpful." (Synovate, 2003). Due to the nature of identity theft, preventing identity theft starts with the consumer. Basic countermeasures can be implemented to deter the identity theft, as they prove to be very opportunistic. Prevention will always start with deterrence, which may be likened to using a video camera or an internal security system on a house in the hopes of preventing burglars. Sure all of these anti-theft devices can be surpassed, but real deterrence comes from actually making the house difficult to steal, so that the thief will eventually move on to the next one. Internet security risks may occur at a variety of levels, users need to setup countermeasures that provide multiple layers of defense against these risks. Users should have the expectation that it is a matter of when they will experience a security problem, not if. Most of the recommended techniques for securing personal information on computers fall into the category of fundamental computer security practices. The following is a breakdown of the methods of prevention for online identity theft:

- Install and regularly update spyware and antivirus on personal computer.
- Install and configure a firewall on personal computer. Having a firewall should hinder identity thieves from getting access to the user's workstation over a network.
- Install and maintain operating system security patches on personal computer.
- Configure security encryption on wireless technologies, such as Wired Equivalent Privacy (WEP) a security protocol.
- Use a secure web browser for online business activities which employ techniques, such as encryption, to keep personal information secure. If the website does not have an padlock image on the browser's status bar or the beginning of the Internet address does not start with https:// it will mean that the site is not secure.
- Block suspicious looking websites.
- Properly check the URL of any site that asks to provide personal information. Users should make sure that their session begins at the known authentic address of the site, with no additional characters added to it.
- Do not store sensitive or financial information on personal computer.
- Users should not select the option to remember identification and authentication credentials or automatically login.
- Log out of websites when finished.
- Log out or shutdown computers when finished.
- Users should practice good password security procedures. Passwords should meet the following complex requirements: Strong passwords should have a combination of numbers, letters, and symbols and use both uppercase and lowercase characters. Users should never write the password down or store in on the computer. Change passwords on a regular basis.
- Beware of email requesting personal information. Never click or reply to a link from an unsolicited email that asks for your credit card, passwords, or PINs, bank account information, social security number or other types of confidential information. When in doubt, contact the financial institution by phone to inquire about whether the request for information is legitimate.
- Before technological devices are disposed of, information should be properly deleted.
- Examine the privacy policies of the financial institutions and companies that have the user's personal information.

Though the importance of online identity procedures is finally being recognized, still more work remains to be done. Information about each individual is quickly becoming an increasingly valuable commodity, and as a repercussion, its management and protection has become a pressing matter. Having global standardization efforts and open source initiatives are critical against identity theft. As of today, no common set of technical standards has emerged. In addition policy and legal considerations require further compliance at the global level.

2.6 – Identity Theft Statistics

"According to Javelin Strategies, a prominent research firm that often reports on identity theft, incidences of the crime increased by 11% from 2008 to 2009 altering the lives of 11 million Americans." (2010) The number of fraud victims continued to rise for the second year in a row. Figure 1 shows a study which was conducted by Javelin Strategy & Research that 11.1 million Americans were victimized last year, with estimated losses exceeding 54 billion dollars. The average loss per complaint was $373. "Those households with incomes higher than $70,000 were twice as likely to experience identity theft than those with salaries under $50,000." (2009)



More Consumers Experience Fraud, but Mean Consumer Costs and Resolution Hours Drop

Overall Measures of Impact

		Survey Report						
	Trend	2009	2008	2007	2006	2005	2004	2003
US adult victims of identity fraud **	↘	11.1 M	9.9 M	8.1 M	8.4 M	8.9 M	9.3 M	10.1 M
Fraud victims as % of US population	↘	4.8%	4.3%	3.6%	3.7%	4.0%	4.3%	4.7%
Total one year fraud amount *	↘	$54 B	$48 B	$45 B	$50 B	$57 B	$60 B	$58 B
Mean fraud amount per fraud victim ***	=	$4,841	$4,858	$5,509	$5,955	$6,436	$6,507	$5,736
Median fraud amount per fraud victim	=	$750	$750	$750	$750	$750	$750	$750
Mean consumer cost	↖	$373	$498	$720	$574	$467	$746	$606
Median consumer cost	=	$0	$0	$0	$0	$0	$0	$0
Mean resolution time (hours)	↖	21	30	26	25	40	28	33
Median resolution time (hours)	=	5	5	5	5	5	5	5

© 2010 Javelin Strategy & Research

Figure 1: Source: More consumers experience fraud, average time to resolve fraud drops, http://gigaom.com/2010/02/10/identity-theft-on-the-rise-survey/, February 10, 2010.

Consumer complaints of identity theft reported to the Federal Trade Commission (FTC) has seen similar increases as well. In 2009, the FTC received 278,078 consumer complaints, despite survey data indicating that 11.1 million Americans were victimized. This discrepancy between research on identity theft and consumer reports could be a direct result of several factors. While some identity theft victims may file a report to the FTC, others may file complaints with law enforcement, while still others may file complaints with credit bureaus. Not all victims filed complaints with consumer protection entities, law enforcement, and credit reporting agencies. Another possible factor contributing to this discrepancy is that victims may not have reported an identity theft incident. These victims may have been more likely to indicate the incident on a survey prompting them about their experiences with identity theft.

The FTC has been recording consumer complaints since 2000. Figure 2 below represents the number of identity theft complaints received by the FTC between 2000 and 2008 in connection to the number of all other fraud complaints received. "According to CRS analysis, since 2000, the number of identity theft complaints has averaged about 37% of the total number of consumer complaints received by the FTC. (Finklea, 2010) Not only has the number of identity theft complaints continued to be the primary consumer fraud complaint to the FTC, but the sheer number of identity theft complaints has generally increased.

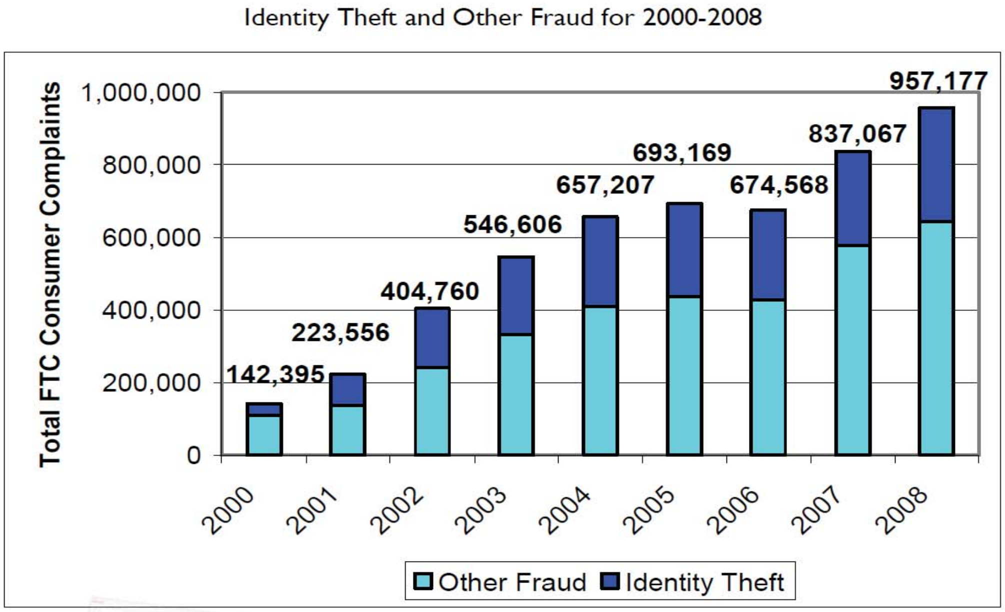


Figure 2: Source: FTC Identity Theft Consumer Complaint data for each calendar year from 2000 – 2008, in correlation to all other fraud complaints. http://www.fas.org/sgp/crs/misc/R40599.pdf, January 10, 2010.

The number of identity theft complaints received by the FTC has generally increased since the FTC began recording identity theft complaints in 2000. Figure 3 below represents the general increase of identity theft complaints reported to the FTC from 2000 to 2008. Since the commission of the FTC began recording identity theft complaints in 2000, the number of identity theft complaints has generally increased.

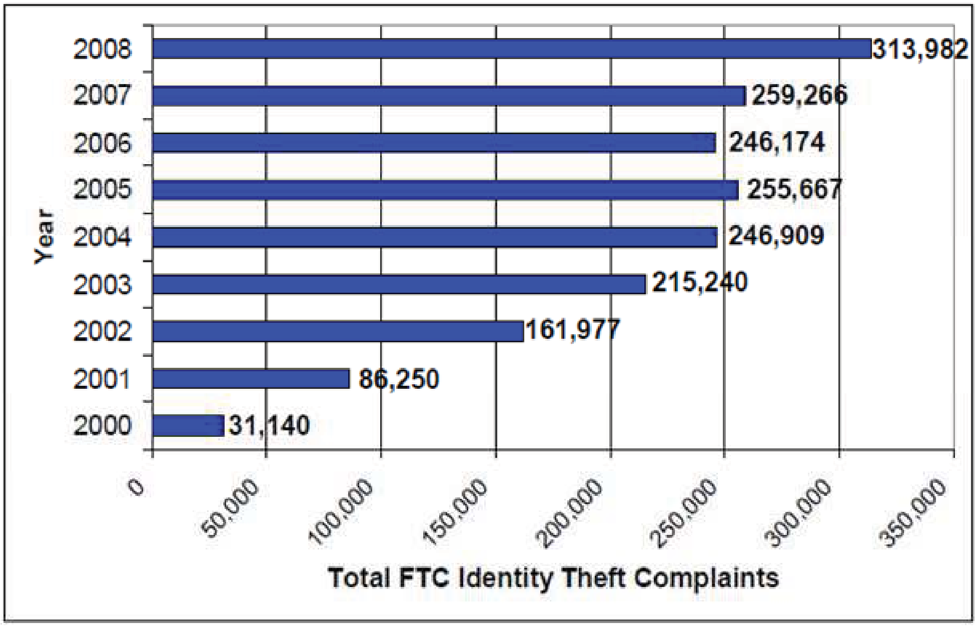


Figure 3: Source: FTC reports an increasing trend in the number of identity theft complaints from 2000 – 2008. http://www.fas.org/sgp/crs/misc/R40599.pdf, January 10, 2010.

Figure 4 provides a brief description of each type of identity theft, which was gathered by the Federal Trade Commission based on complaint data.

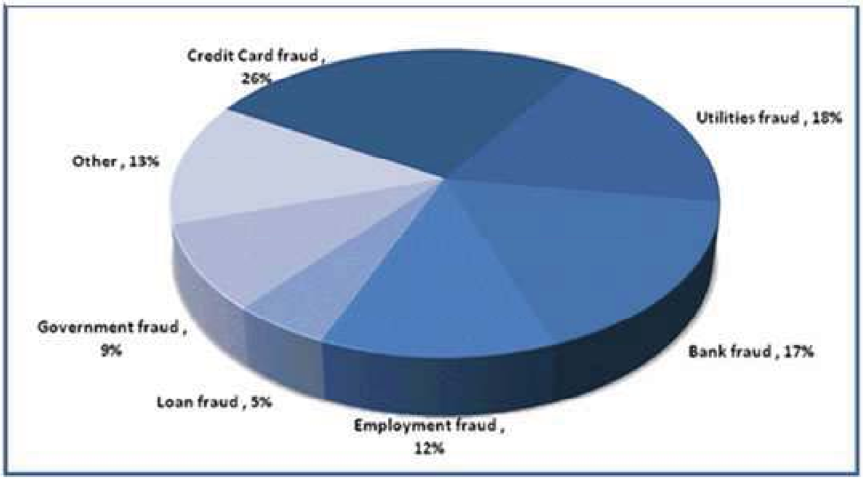


Figure 4: Source: Types of identity theft statistics in 2009. 2009. http://www.spendonlife.com/guide/2009-identity-theft-statistics, 2009.

- Credit Card fraud (26%): Credit card fraud continues to be one of the most common of identity theft reported by victims. This can occur when a perpetrator acquires the victim's credit card number and uses it to make a purchase.
- Utilities fraud (18%): Utilities are opened using the name of someone who may not be living at the residence. Parents may be so desperate for electricity, water, and gas that they would use their own children's clean credit report to be approved for utilities.
- Bank fraud (17%): Many forms of bank fraud, including the following: ATM pass code theft, check theft, and changing the amount on a check.
- Employment fraud (12%): This will occur when the perpetrator does not have a valid social security number and steal a victim's to obtain a job.
- Loan fraud (5%): Loan fraud occurs when the perpetrator applies for a loan in the victim's name.
- Government fraud (9%): This type of fraud will include the following: driver license, tax, and Social Security fraud.
- Other (13%)

The FTC not only shows that identity theft is rising, but that it is targeting one of most financially vulnerable age groups: 20-29 age groups. Over the past three years, the target demographics for identity theft have remained the same.

> In 2006, the 20-29 age group made up 25-percent of the complaints, while the 30-39 age group made up 23-percent. In 2007, the two groups were at 24-percent and 23-percent, respectively, and, in 2008, at 24-percent and 23-percent." (Hwang, 2009)

The belief is that identity thieves are targeting victims with expendable income and have less experience in dealing with identity theft scams. Figure 5 displays, in 2009 again these numbers continue to stay roughly the same. According to the FTC, 65 percent of the complainants were between the ages of 20 and 49. Nearly half (46 percent) of the victims were between the ages of 20 and 39. The largest numbers of complaints were collected from Florida, Arizona, Texas, California, and Nevada. North Dakota reported only 192 complaints in 2009, ranking 49th out of 50 states.

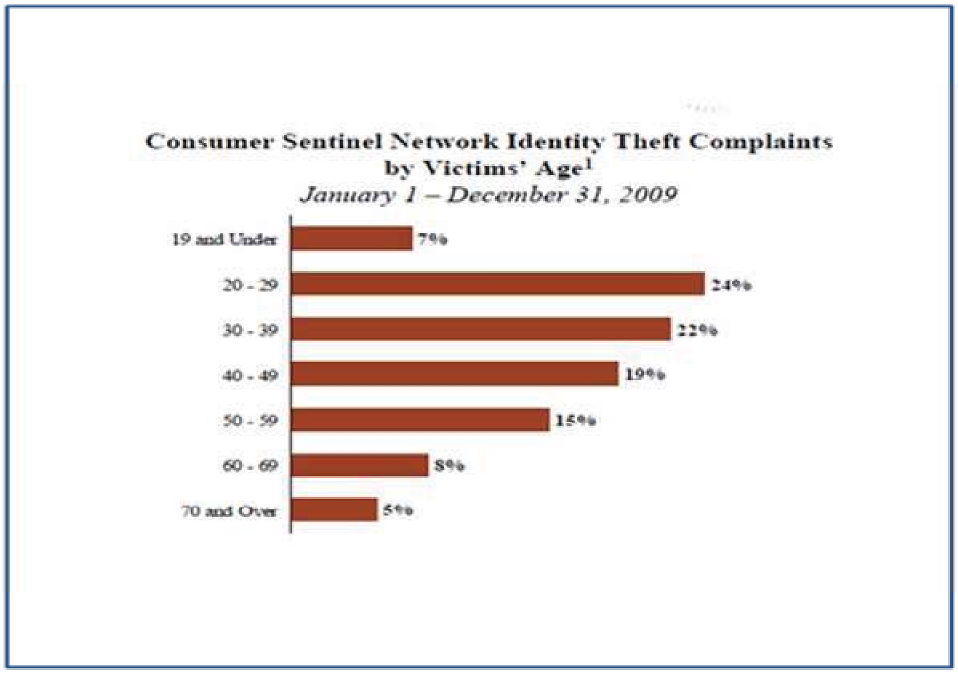


Figure 5: Source: Consumer Sentinel Network Identity Theft Complaints by age in 2009. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf, February 2010.

The perception may that identity theft only occurs when the identity thief is across the world that may be sending out a fraudulent email, but this is not the case. 43% of the time victims claim that identity theft occurred when someone they knew used their personal information inappropriately. Many victims claim that the perpetrator is someone they know who feels some animosity or anger towards them. "Of identity theft cases where the perpetrator was identified 13 percent were cases of "friendly theft," perpetrated by friends, family members, or in-home employees." (2010) Relationships that were identified included family members, neighbors, roommates, co-worker, or individual's working in the victim's home.

2.7 Victims Experiences and Rights

Victims of identity theft often experience financial losses in addition to non-monetary harm. The leading types of non-monetary harm cited by victims were invaded privacy, time to resolve problems, denied credit or other financial services, and lack of closure. Some victims also claim that they have been subjected to criminal investigations, arrests, or convictions of identity theft related crimes. "It has been estimated that in every 30 to 60 hours a victim handles various matters, which are related to cases of stolen identity which includes creating an account or using existing accounts." (DeJarnette, 2009) Victims also believe that (1) that they receive little help from authorities who announced the identifying information to them; (2) that they receive the proper support from the credit reporting agencies, banks, or the credit guarantors; (3) that law enforcement agencies did not properly investigate many identity theft crimes due to the lengthy number of complaints.

Many news reports signify that people everywhere are increasingly being fooled by identity theft. Identity theft victims continue to be the focus of this crime in television interviews and news articles, while the justice system generally focuses on the perpetrators. Some of the stories include:

I. "What the Wilkinsons believe may have been months after his wife fell victim phishing attack, the couple began noticing that their online banking transactions were not going through. Automatic bill payments were being turned down for insufficient funds and checks were being ordered and mailed to locations the Wilkinsons did not recognize. At one point, the fraudsters tried to wire a $40,000 line of credit from the Wilkinsons' account. "It puts you in a terrible place, and you don't know what do," Wilkinsons says." (Kitten, 2010)

II. "Parents, pay especially close attention to this unfortunate identity theft story. These days, ID theft victims are getting younger and younger. The Consumerist reports that a thief stole the identity of 9-year-old Kyle Shoemaker to open up two credit card accounts and an $18,000 line of credit. Apparently, ID thieves don't discriminate against age." (2007)

III. "One 23-year-old Delaware waitress was paid $10-$15 for every card she skimmed. A similar scam in Los Angeles was discovered after six customers complained of $16,000 in unauthorized charges. All, it turned out, had dined at the same restaurant." (Handsschuch, 2009)

While most financial organizations do not hold victims accountable for fraudulent debts, victims may incur a substantial amount of expenses while trying to restore their financial health and good name. It has been reported by the FTC, that victims may incur costs on a routine basis on the following items: notary fees, document copies, certified mail, and long-distance telephone calls. In some cases, victims may have had their tax refunds withheld pending resolution of the identity theft crime. "Respondents in 2009 spent an average of $527 dollars in out-of-pocket expenses for damage done to an existing account." The average out of pocket expenses have declined from $741 which was reported in 2008. (2010) The FTC also reported that out of pocket costs of identity theft victims varied widely.

> However, 10 percent of all ID theft victims reported costs of $1,200 or more, and 10% of victims of new accounts and other frauds reported out of pocket costs of $3,000. One quarter of all new accounts victims reported expenses of at least $1,000. (Frayer, 2009)

The Identity Theft and Assumption Deterrence Act in October of 1998 became the first piece of federal legislation to deal directly with identity theft. The act was necessary because prior to its enactment, laws only addressed the fraudulent creation, transfer or use of identification documents. This legislation makes identity theft a federal crime with penalties up to 15 years incarceration and a maximum fine of $250,000. This act makes it a crime when a perpetrator performs the following:

> knowingly transfers or uses, 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. (2008)

This Act established the Federal Trade Commission (FTC) as the government body charged with establishing procedures to log and acknowledge the receipt of complaints by victims. The FTC will then provide educational materials to these victims and to refer the complaints to the appropriate law enforcement agencies and three major national credit reporting bureaus.

The Electronic Fund Transfer Act (EFTA) of 1978 is devoted to protecting consumers engaging in electronic fund transfers (EFTs). EFT services may include the following: transfers through automated teller machines, debit cards, automated clearinghouse systems, point of sale terminals, and telephone bill payment plans. This Act also limits the debt for unauthorized electronic fund transfers. The amount of loss that the victim incurs is responsible on how quickly the stolen or lost ATM or debit card is reported. If the card is reported stolen or lost within two business days, the victim will be liable for a maximum of $50 for the total losses incurred. If the card is reported is reported to the financial institution between a 3 and 60 day timeframe, the victim will be liable for up to $500. If the victim waits until after 60 days, the victim will be liable for all of the money taken out of their account and before the card was reported missing. MasterCard and VISA took the initiative to limit the victim's liability for unauthorized purchased of a debit card to $50 per card, no matter how much time has elapsed since the discovery of the theft or loss of the card. It is advised that if a fraudulent transaction is identified, in addition to calling the financial institution, follow that up in writing with a certified letter, return receipt requested. After being notified of an error on a statement, the financial institution has 10 business days to investigate. After the investigation has been completed within three business days all error must be corrected after determining that an error has occurred.

Fortunately, the victims of identity theft do have some assurances related to financial losses. The Truth in Lending Act (TILA) is a federal law which was instituted by Congress in 1968, regulates the extension of consumer credit by lender in the United States. “This federal law aims at protecting the public against unfair and erroneous credit card practices and credit billing.” This Act has the following several provisions: Limits the amount the cardholder can be charged for unauthorized purchases, Blocks credit card companies from issuing cards to individuals who have not applied for them. In most cases, TILA limits liability for unauthorized use of credit card charges up to 50 dollars to credit card holders.

“A federal law called the Fair Credit Billing Act gives people who use “open end” credit accounts the right to dispute fraudulent and unfair credit charges.” (2010) Effective in 1975, the Fair Credit Billing Act (FCBA) requires that a credit card company immediately credits the identity thefts victim’s payments and adjusts mistakes on their bill. To take advantage of the law’s consumer protections, write to creditor at the address given for “billing inquiries”, and include your name, address, account number, and a description of the billing error. The victim should mail their letter so that it reaches the creditor within 60 days after the first bill containing the error was mailed out. Even if there is a case that the identity thief changed the address on the account and the bill was not received, the dispute letter still must reach the creditor within 60 days, or the victim may be responsible for the charges. When the victim sends a dispute letter, this should be sent by certified mail with a request for return receipt. It is then the creditor’s responsibility to acknowledge the complaint in writing within a 30 day time frame, unless the problem has been resolved.

Chapter 3 – Methodology

Most of the secondary research tools that will be utilized will be the following: The library and its resources, World Wide Web, news, computer periodicals, and surveys. A number of case studies or victim testimonials on the subject of identity theft can be located within congressional hearings. A structured survey was used as a research instrument. This sample study will be based on a non-probability planned sample of colleagues from my place of employment. Existing surveys may be referenced with regards to their methodologies, population estimates, and sample sizes. The survey will be conducted and any modifications that are necessary will be made to the questions.

Creating a model for a given domain from scratch can be very difficult and time consuming. One of the major ontologies that will be utilized is the quantitative research method. Information from standards and classification schemes that already exist will be utilized as well as case studies, news articles, books, and websites. The proposed methodology used for building computer fraud ontology should be treated through a risk management process. The focus of risk management is to identify, measure and consider these risks in order to reduce the likelihood of identity theft happening. Establishing the fraud relations for a home user involves defining the type of fraud the home user wishes to fight and identifying which processes that fraud occurs upon. The computer fraud ontology will be a generic framework for defining both the domain and case specific fraud ontologies. This framework will be able to adapt and extend to different domains and types of fraud.

The Interpretivist Epistemology will be employed. In the field of computer security there are multiple ways to get the job done. Having virus protection installed on a computer can provide a good level of security, but having a firewall and antispyware applications installed can provide a stronger sense of security. Having a layered approach is the best defense on protecting users from computer identity theft. Hackers may be able to easily get past one layer of defense, but by employing multiple layers, this will make life more difficult for hackers as they try to invade your information.

The thesis will be made more manageable in the following ways: focus will be placed on educating users on some of the ways identity theft occurs, implement common security practices to circumvent a security breach, and discuss the existing laws in place to protect users. By setting up these parameters, this should provide a framework for my thesis research. "

> By way of comparison, identity theft-related losses due to credit card account takeovers at the two largest credit-issuing organizations totaled $46.1 million in 2000, and total check fraud-related losses associated with new-account fraud, check forgery, unauthorized access to checking accounts, illegal credit card purchase, and fraudulent cash advances on credit cards, collectively, were estimated to total $2.4 billion over the 12 months ending April 2004, or $1,200 per victim. (2004)

People should find this research interesting because if computer identity theft continues to grow, the growth of online banking and commerce will gradually decline. Experts recommend using a layered approach to computer security because no single security method is sufficient to prevent identity theft. By educating consumers to practice some common security practices, consumer confidence may rise on how it may come to trust online transactions which may help all participants in Internet commerce.

The bulk of my research will come from secondary research. With that being said, repetitive patterns should start to materialize with what is being read. Once these patterns start to become more familiar, then it will be time to conclude the literature review research.

Chapter 4 –Results

4.1 Research Questions

This survey was designed to answer certain research questions to determine the extent of the prevention of identity theft. Questions 1 – 2 were focused on a respondents experience with identity theft.

1. Have you ever been a victim of identity theft?

    ○ Yes
    ○ No

2. Do you know someone that has been a victim of identity theft?

    ○ Yes
    ○ No

Questions 3-5 focused on capturing the demographic information from the respondents. The purpose of this was to determine if there was a segment of the population that were affected more so than the other(s) by identity theft.

3. What is your sex?

    ○ Male
    ○ Female

4. Please specify your race.

    ○ American Indian or Alaska Native
    ○ Asian
    ○ Black or African American
    ○ Hispanic or Latino
    ○ Native Hawaiian or Other Pacific Islander
    ○ White

5. What is your age range?

    ○ 18-29
    ○ 30-39
    ○ 40-49
    ○ 50-60
    ○ 61+

Question 6 wanted to ask the respondent's opinion on whether they felt identity theft will increase or decrease in the near future.

6. Identity Theft is likely to increase rather than decline in the near future.

    - Strongly Disagree
    - Somewhat Disagree
    - Somewhat Agree
    - Strongly Agree

Question 7 focused on capturing the respondent's computer usage. Due to the continued uptick in Internet usage, this will further expose respondents to identity theft.

7. Do you use a computer at your workplace, at school, at home, or anywhere else on at least an occasional basis?

    - Yes
    - No

Question 8 was asked to determine the frequency of respondent(s) reading any disclaimers before downloading or installing any programs. If respondent(s) read through the disclaimer, malware may be minimized from being downloaded onto a computer.

8. On a different topic…how often, if ever, do you read user agreements, privacy statements, or other disclaimers before downloading or installing programs or files from the internet?

    - Always
    - Most of the time
    - Only sometimes
    - Hardly ever
    - Never

Question 9 was designed to capture how respondents may be using the Internet. Some of these possible ways may be how respondent's contract malware onto their computers.

9. Please tell me if you ever use the internet to do any of the following things. Do you ever…?

   Please select all that may apply.

   Send or read e-mail
   Buy a product online, such as book, music, toys, or clothing
   Play online games
   Share files from your own computer, such as music files
   Download music files onto your computer so you can play them at any time you want
   Download computer programs from the internet
   Visit an adult website

Questions 10 – 13 focused on the respondent's experiences to spyware on their computers. Respondents may be aware of the danger posed by malicious files found during normal web surfing activities, but they may still be unaware of spyware and the dangers they pose until they get infected. These questions were asked to determine the potential of the respondents having been affected by spyware possibly without their knowledge.

10. In the past year, have you experienced any of the following problems on your main home computer, or not?

    Your computer has slowed down or is not running as fast as it used to.

    - Yes
    - No

11. Your computer started freezing up or crashing, requiring you to shutdown or reset.

    - Yes
    - No

12. Your internet home page changed without you resetting it.

    - Yes
    - No

13. A new program appeared on your computer that you didn't install or new icons suddenly appeared on your desktop.

    - Yes
    - No

Question 14 wanted to capture the respondent's opinion of their ability to keep malware off of their computers. The question was asked to track the respondent's belief in their ability to combat the problem.

14. Overall, how confident are you that you can keep things like computer viruses, spyware, and adware off of your home computer when you want to?

    - o Very Confident
    - o Somewhat Confident
    - o Not Too Confident
    - o Not At All Confident
    - o Do Now Own A Home Computer
    - o Do Not Know

Question 15 wanted to track if the respondents have experienced phishing scams. Respondent's that unknowingly give out their username and passwords may have their accounts raided by identity thieves.

15. Have you ever been prompted by an email from your financial institution to enter your password information to gain access to your account?

    - o Yes
    - o No

Question 16 wanted to track to see if respondents had virus protection software installed on their computer. This question was posed to see if the necessary steps are taken in hopes of mitigating a respondent's risk.

16. Do you happen to have virus protection on your main home computer?

    - o Yes
    - o No

Question 17 wanted to capture the frequency of how often a respondent will update their virus definition file. Antivirus applications are only as good as the most recent virus definition file update. The most recent updates will likely protect respondents from being attacked by the latest virus.

17. How often is the virus protection on your main home computer usually updated?

    - o Daily
    - o Weekly
    - o Monthly
    - o Do not know

Question 18 wanted to capture if respondents have firewalls installed on their computers. Respondent's that use good Internet firewalls; continue to protect themselves from the spread of hacker dangers, often without being aware of it.

18. Do you happen to have a firewall installed on your home computer?

○ Yes
○ No

Question 19 wanted to capture the respondent's confidence in protecting themselves from identity theft. The Internet has drastically transformed the way personal details, income, and expenses are handled.

19. Do you know what to do to protect yourself against identity theft?

○ Yes
○ No

Question 20 is asked to see if the respondents practice any of the security tips that are listed below. By applying an onion layered approach to security, respondent's can make their computers more difficult to penetrate when it comes to identity theft.

20. Do you practice the following security tips on your home PC or laptop?

Please check all that apply.

Install and maintain Operating System patches.
Install and regularly update AntiVirus and AntiSpyware applications.
Install and configure a firewall on personal computer.
Configure security encryption on wireless technologies
Use strong passwords.

4.2 Initial Survey

The awareness of identity theft survey was originally designed and administered as a study for a research methods class. This pilot study was initially disseminated to 110 engineers within my company of Aurora, CO 2010. Since the researcher was already employed with the engineering firm in Aurora, the respondents were chosen as a convenience sample, because they were readily available to take the surveys. An online survey was created and distributed by email, which the user could gain access by clicking on a link. The main focus of the Identity Theft survey was to obtain quantitative data regarding identity theft awareness.

Emails were distributed to 110 engineers among various age groups at Merrick & Company in Aurora, CO. The age ranges from 18-29, 30-39, 40-49, 50-60, and 61+. To avoid duplication, engineers were encouraged to complete one survey, and a setting in the online survey was checked off allowing one response per computer. Respondents could not go back and change existing responses after the survey is submitted. Each survey that was submitted also tracked the respondents IP address of the computer that they were on. Although this did not occur, any responses that had a duplicate IP addresses would be tossed from the data collection.

Part of the survey was designed for quantitative purposes and asked for personal experience either as a victim of identity theft or did they know anybody who may have become a victim. This survey also requested demographic information, such as the following: age, race, and sex. All 110 respondents reported to this question. The next part of the survey asked for Yes\No responses or chose multiple answers in a multiple choice setting. The results of this survey produced outstanding results.

This study targeted the engineering population at Merrick & Company, but ultimately identity theft can affect anybody. The estimated 2009 US population was 307,006,550. Javelin's research showed that 11 million people were victims of identity theft in 2009, this represents that 3.6 percent of the US population have been victimized.

Table 1

Engineers at Merrick & Company

	18-29 engineer	30-39 engineer	40-49 engineer	50-60 engineer	61+ engineer	Total
American Indian or Alaska Native	0	0	1	1	0	2
Asian	0	1	1	0	0	2
Black or African American	8	8	3	9	2	30
Hispanic or Latino	2	2	3	0	0	7
Native Hawaiian or Other Pacific Islander	0	0	0	0	0	0
White	10	18	13	23	5	69
Totals	20	29	21	33	7	110

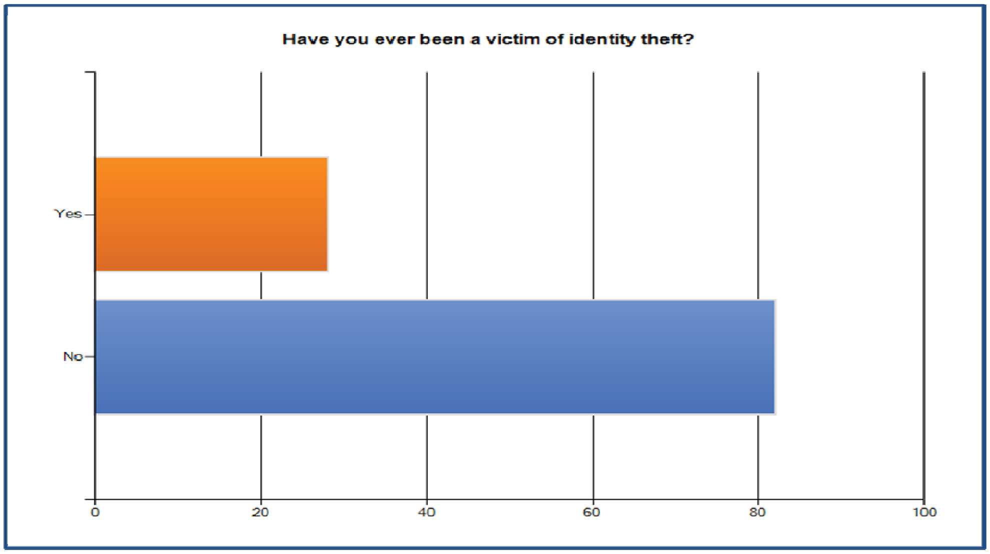
Surveys were distributed to 110 employees of Merrick & Company. Prior to distributing the surveys, approval was requested from project management of each department. Merrick has a lot of diversity among all departments throughout the company. The number of surveys to distribute was calculated based on the populations chosen. 55 males and 55 females were polled totaling 110 employees. This represents that 22 percent of the organization was polled, as the total employee count for full time employees at the main headquarters of Merrick & Company in Aurora, CO totaled 500. All of the surveys that were forwarded to Merrick employees were returned (100% return rate). The data was collected from the surveys which were compiled into an Excel workbook.

4.3 Prevention of Identity Theft Survey Results

The first section of the survey of identity theft prevention asked five personal questions about the respondents. In section 4.1, question 1 provided two responses from which to choose. 28 out of 110 respondents admitted to being victimized by identity theft. Most of these victims were white males that were in the 40-49 age range.

Table 2

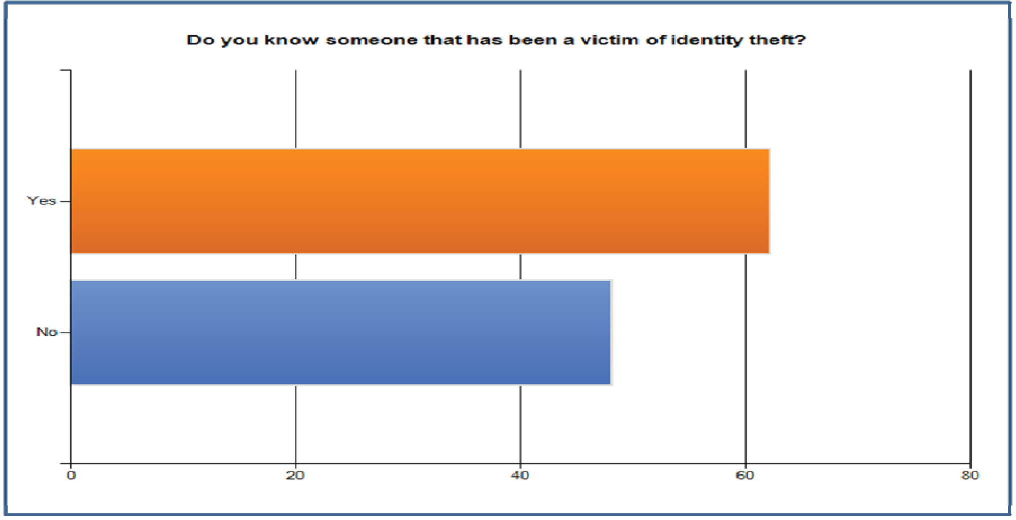
Question 1: Have you ever been a victim of identity theft?



Section 4.1, question 2, provides two possible responses between male and female. 62 out of 110 respondents knew someone that has been victimized of identity theft.

Table 3

Question 2: Do you know someone that has been a victim of identity theft?

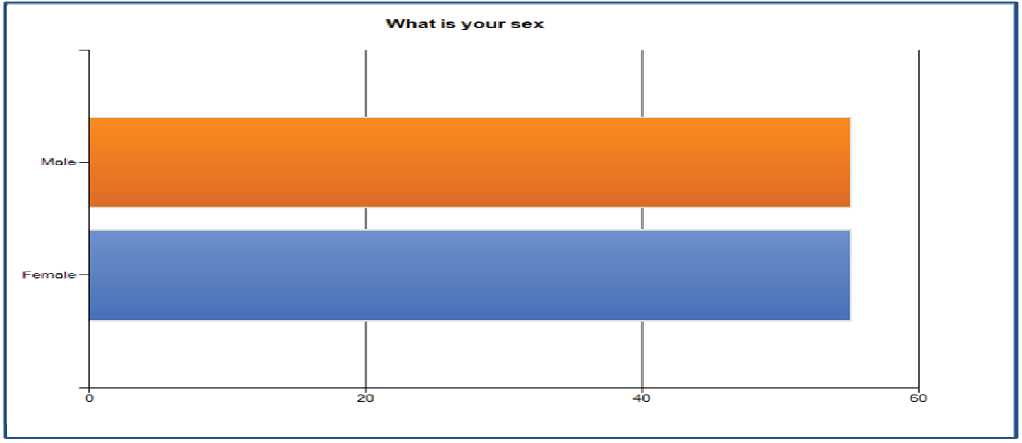


57 million Americans receive scam emails on an annual basis. “19% click on the link inside. 3% disclose bank and financial information by accident. 1.7% is then scammed.” (2010)

Section 4.1, questions 3 -5 captures demographic information. Section 4.1, question 3, respondents had two responses to select from between Male and Female. 55 males and 55 females were polled.

Table 4

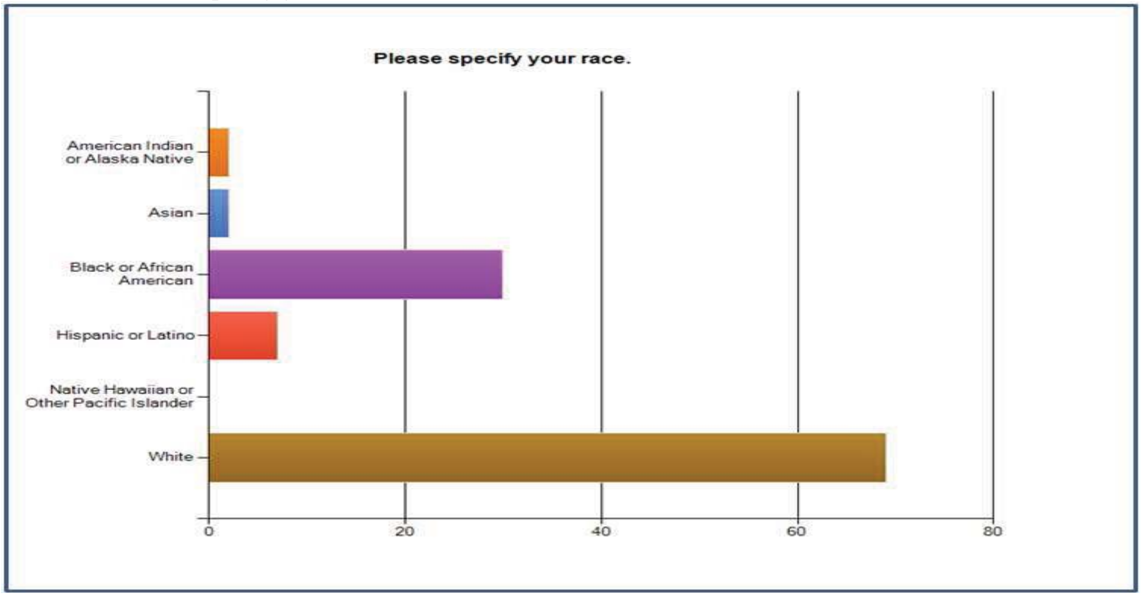
Question 3: What is your sex?



Section 4.1, question 4 had the following 6 choices to choose from: American Indian or Alaska Native, Asian, Black or African American, Hispanic or Latino, Native Hawaiian or Other Pacific Islander, or White. The majority of the respondents were white representing 62.7% of this survey.

Table 5

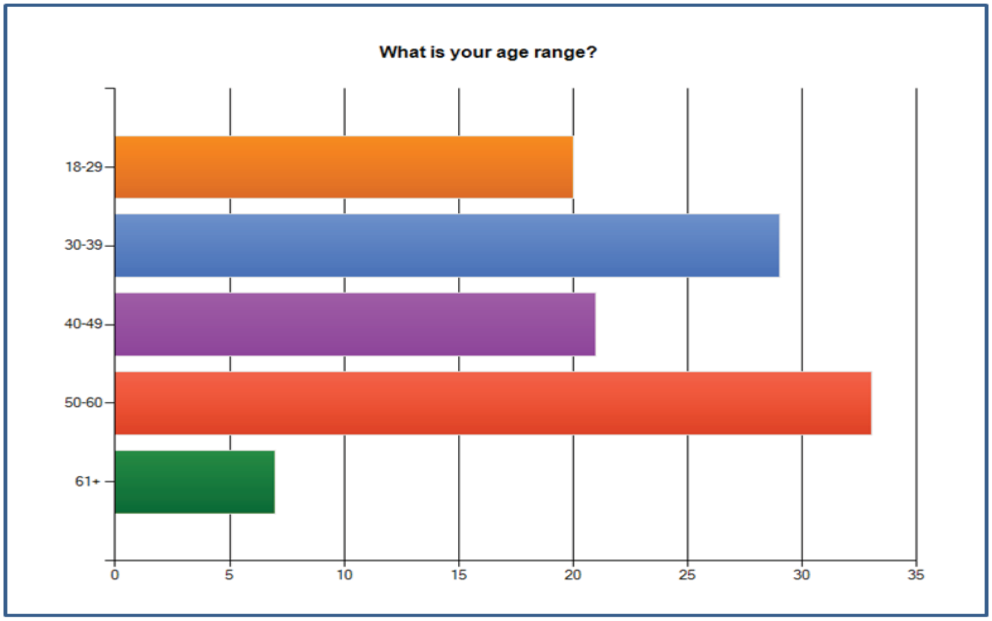
Question 4: Please specify your race.



Section 4.1, question 5 had the following 5 choices to choose from: 18-29, 30-39, 40-49, 50-60, and 61+. The majority of the respondents were in the 50-60 age range representing 30% of the engineering population.

Table 6

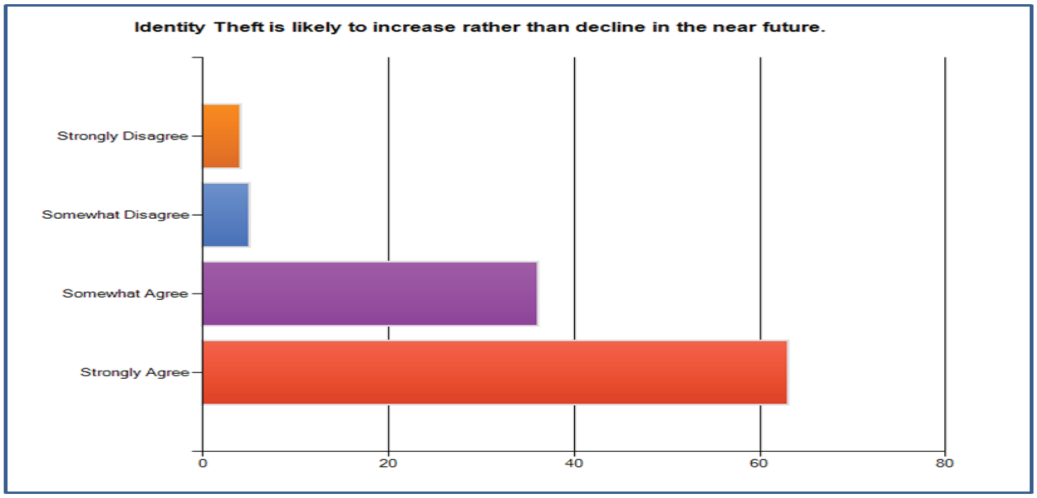
Question 5: What is your age range?



Section 4.1, question 6 had 63 of 108 respondents strongly agreed that identity theft would increase in the near future. 2 respondents skipped this question.

Table 7

Question 6: Identity Theft is likely to increase rather than decline in the near future.



Nationally recognized experts in identity theft have come up with 10 predictions for what the nation can expect in 2010 and beyond.

I. **More Scams:** Whenever there is a difficult time within the United States, perpetrators will find a way to take advantage of the existing problem. Today there are more variations of sophisticated new scams.

II. **Job Scams:** With the unemployment rate holding at an all time rate of 9.6%, perpetrators are taking advantage of this by tricking desperate people seeking out employment. Fake work at home scams or job listings will lead to the victim providing their Social Security number.

III. **New Low Tech "Desperate" Identity Theft:** More perpetrators are beginning to explore the crime of identity theft for quick money.

IV. **All-in-the-Family ID Theft:** During tough economic times, it has been well documented that a considerable amount of identity theft cases are perpetrated by people close to the victim.

V. **Child Identity Theft:** It has come to realization that a child's SSN may be used for more than opening a line of credit.

VI. **Medical Identity Theft:** Perpetrators may hack into a database or break into medical facilities to line their own pockets. Information may be stolen by employees at medical facilities and resold on the black market.

VII. **Insider Identity Theft:** Highly skilled perpetrators may be able to take advantage of a lack of security measures which may lead to financially harmful breaches.

VIII. **Governmental Identity Theft:** Individuals o identity theft may realize that they have become victimized as they applied for government benefits or assistance. The victim may be denied benefits temporarily due to the fraudulent use of their child's SSN, in addition to their own SSN being used.

IX. **Criminal Identity Theft:** This type of identity theft related crime will continue to grow. Perpetrators will use a victim's personal information to avoid charges having being tied to their own criminal record.

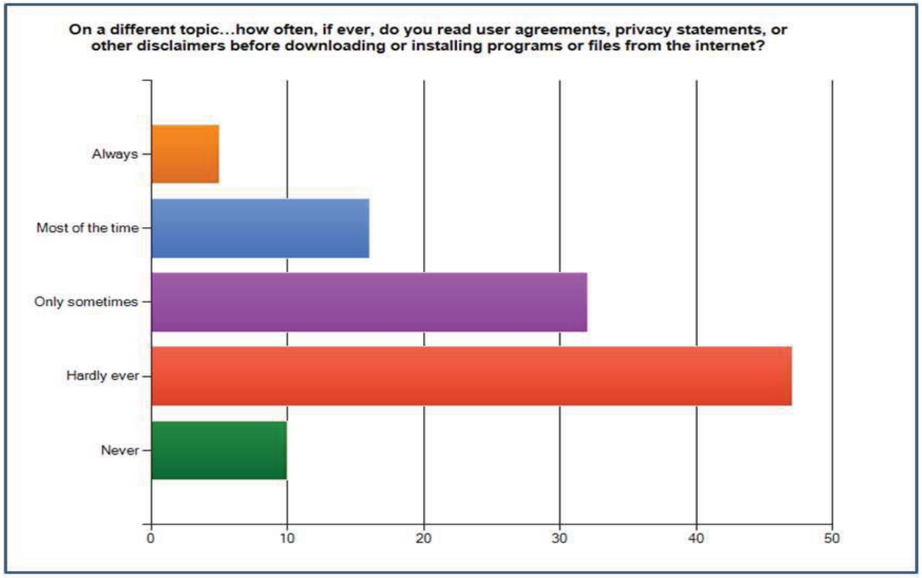
X. **Social Media Identity** Theft: This social media tool has served as a launching pad for identity thieves. "Tainted Twitter and Facebook updates are riddled with spam and viruses in status posts where links are often disguised in short URLs that go to spoofed sites or include a downloadable virus." (Siciliano, 2010)

Section 4.1, question 7 had 107 respondents answered yes. 3 respondents elected not to answer this question. Computers are used in each and every aspect of life. Browsing the internet is the most common computer related use. Users may use the internet for research purposes, email, discussion groups, downloading files, games, education, dating, news, job hunting, and shopping. As of June 2010, 77.3 of the US population use the internet.

Section 4.1, question 8 had 47 out of 110 respondents hardly ever read the documentation before downloading or installing programs from the internet.

Table 8

Question 8: Do you read user agreements, privacy statements, or other disclaimers before Downloading or installing programs or files from the internet?

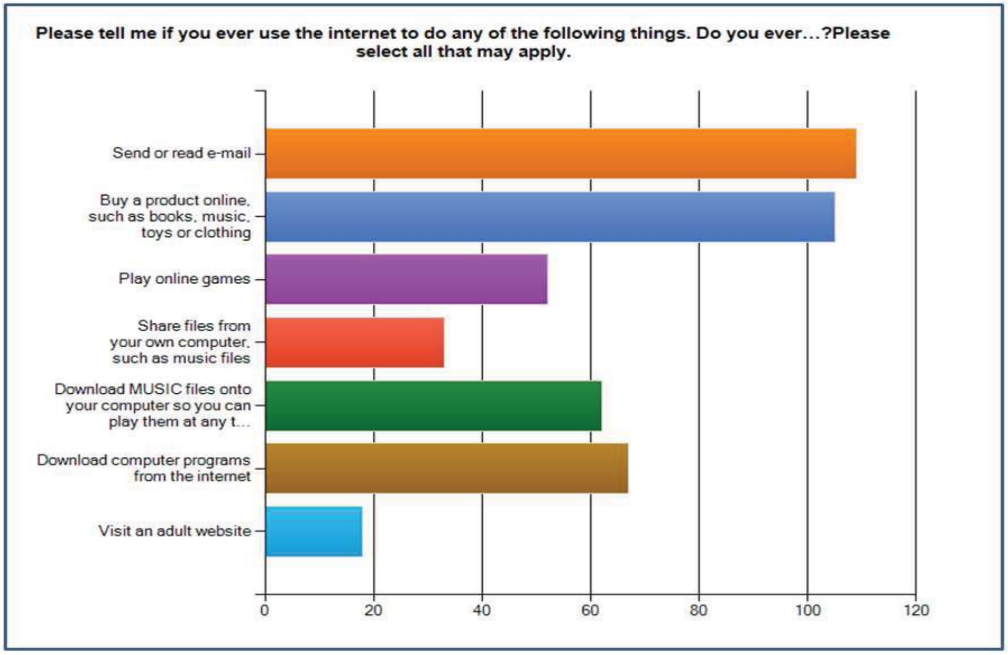


Spyware usually gets on personal computers by attaching itself on other software applications, particularly some free software that could be downloaded from the Internet. "The web server may maintain customary records of the user's IP address, the date and time of access, and will record the search query made by the user for the purpose of generating aggregate search statistics." (2010) Often this example is stated in the user agreement on whether or not additional software will be installed, but most users do not take the time to read the fine print. It is important that the user understands what types of programs are being downloaded and that the user agreement is read before accepting any software.

Section 4.1, question 9 had 109 out of 110 respondents chose send or read email as the number one task that is performed on the internet.

Table 9

Question 9: Please tell me if you ever use the internet to do any of the following things. Do you ever…? Please select all that may apply.



As shown with the survey results, most people incorporate online computing into their lifestyle in some fashion. Viruses may be downloaded from various applications on the internet. The first type of email based threat was recorded in1999 when the Melissa virus struck. Instead of transferring a virus from PC to PC via floppy disks, now new malware can be spread by using the speed and efficiency of network communications. Viruses are placed in emails in and the email receipt has no idea that anything is wrong until the damage has been done. In order for a virus to infect the computer, the attachment must be opened. If any email looks suspicious in any way, users should not open the email message or download the attachment.

In recent years, more people have found the internet as a convenient way to shop online. The world of e-commerce has expanded our purchasing power from local retailers to worldwide organizations. Sometimes things may go wrong in cyberspace, where online shoppers are cheated by identity thieves. Perpetrators aiming to steal the victims account and financial information are increasingly using phishing tactics disguising themselves as web companies like eBay or Amazon. These sites that may seem authentic in fact will capture credit card numbers of unguarded shoppers. The perpetrators may then use the stolen credit card numbers to make purchases in the victim's name. The most frightening part is that users do not need to enter their information on the fake website to become a victim. Identity thieves are now embedding data stealing spyware that downloads to the user's computer as soon as they click on one of the embedded links in an email.

High speed internet connections and new technologies have helped online gaming become a popular pastime on the internet. Today gamers spend a lot of money and time on sophisticated games, while perpetrators see the opportunity for illicit profit. One popular genre of video games that has come to the forefront is Massive Multiplayer Online Role Playing Games (MMORPGs). This will allow gamers to customize their own online identity as game characters who participate in virtual adventures which sometimes may intersect with the real world. "In some games, there is a user-created, virtual world where people use real money to create or purchase personal property in their online world." (Hayes, 2008) This has created a new opportunity for identity thieves called virtual crime. When playing online video games, users that install executable addons may subject themselves to viruses or keyloggers that steal their login information. If a perpetrator can gather information about the victim from their profiles that were created, they may be able to establish accounts in victim's name or use it to gain access into their financial accounts.

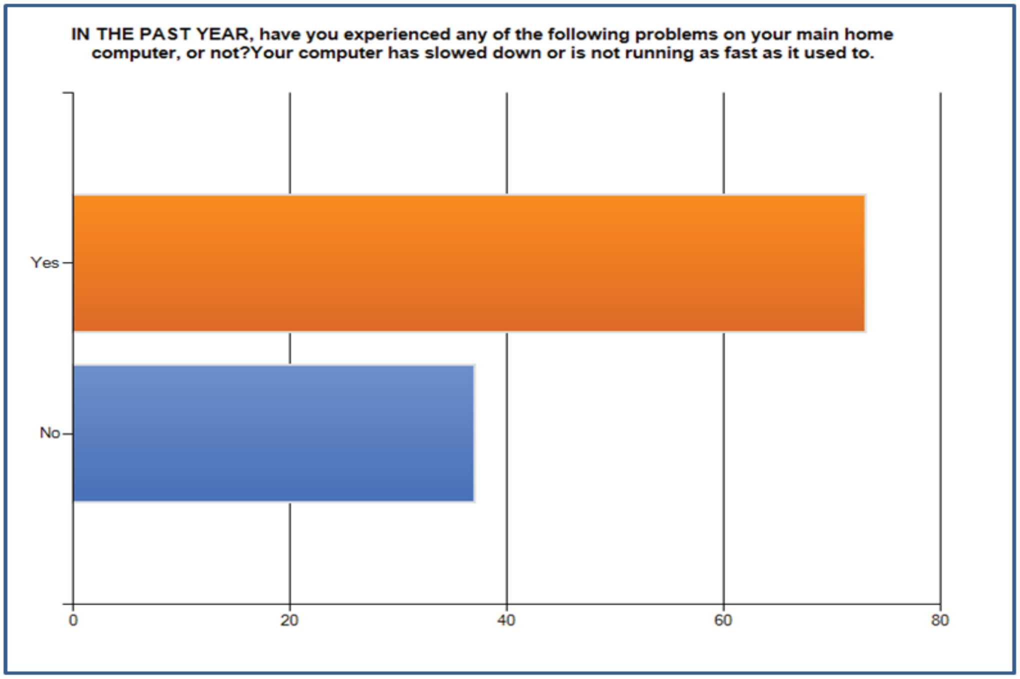
The internet has become a common place to share information such as music, movies, and software downloads all possible through the use of Peer to Peer (P2P) file sharing between computers. File sharing is executed by using software which allows the users to save downloads in a designated folder and also shares files they have with other user's online. Viruses and spyware is common and this will serve as an excellent path for obtaining personal details from a victim's computer and committing identity theft. Certain files when downloaded from P2P networks may have spyware attached to them when the file is opened, the spyware is installed and it can set about analyzing through personal folders to extract personal information about the victim to send back to the identity thief. P2P also opens ports on the user's computer. These ports serve as an avenue which allows data in and out of the computer that flow to and from the internet. Ports are open for the purpose of P2P, but other ports may be opened where the user is not aware of. Programs such as Limewire have been used to search computers of others who were part of a P2P network, for tax returns and credit reports that have been stored electronically.

The online adult business is a multi-billion dollar industry. Some members of the engineering organization have indicated that adult websites have been visited. Adult websites have been notorious for downloading spyware onto a user's computer and some of it is malicious. In 2009, Google has found that 2% of all adult websites contain malicious code that will attempt to compromise a user's computer. Some porn sites may trick the victim into downloading spyware or viruses on their computer. A site may prompt the victim to download an Active-X component to make the site work correctly. If the victim agrees to the download and installs it, they may actually be downloading a type of spyware or virus. Other adult websites may redirect a victim to malicious pages that have viruses on them and will infect their machine instantly. The majority of adult websites will use pop-ups to collect information and money from users who browse free pornography. This information can be sold or misused for identity theft.

Section 4.1, question 10 had 73 out of 110 respondents answered yes to this question.

Table 10

Question 10: In the past year, have you experienced any of the following problems on your main home computer, or not? Your computer has slowed down or is not running as fast as it used to.

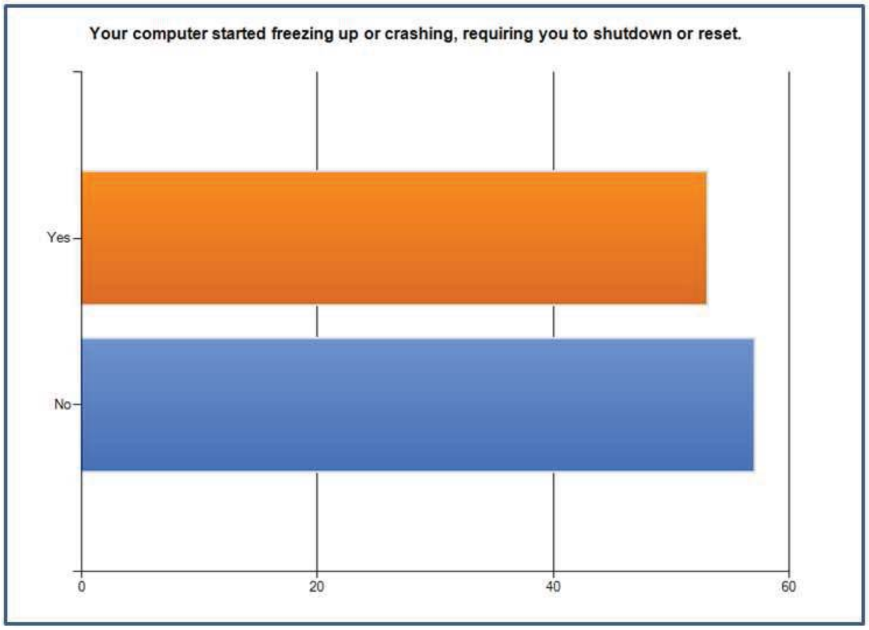


Most people view spyware as simply being a nuisance. If spyware is left unchecked and dealt with occasionally, this can permanently impact the user's computer's ability to run smoothly. User's that pay thousands of dollars for a nice computer and accompanying software have the high expectation of top notch performance out of their investments. Spyware is one of the things that can halt performance to a crawl. Typically, spyware will utilize a lot of resources to track the user's activities and deliver advertisements that will bog a computer down. Spyware slows down computer performance by taking up system resources such as the following: memory space, CPU time, disk space, and internet bandwidth. By clicking on certain popup windows, or downloading free utilities, games, or toolbars, there is a pretty good chance that spyware may have attached itself to a user's computer. The most common source of spyware is file sharing from P2P networks.

Section 4.1, question 11 had 57 out of 110 respondents answered no.

Table 11

Question 11: Your computer started freezing up or crashing, requiring you to shutdown or reset.

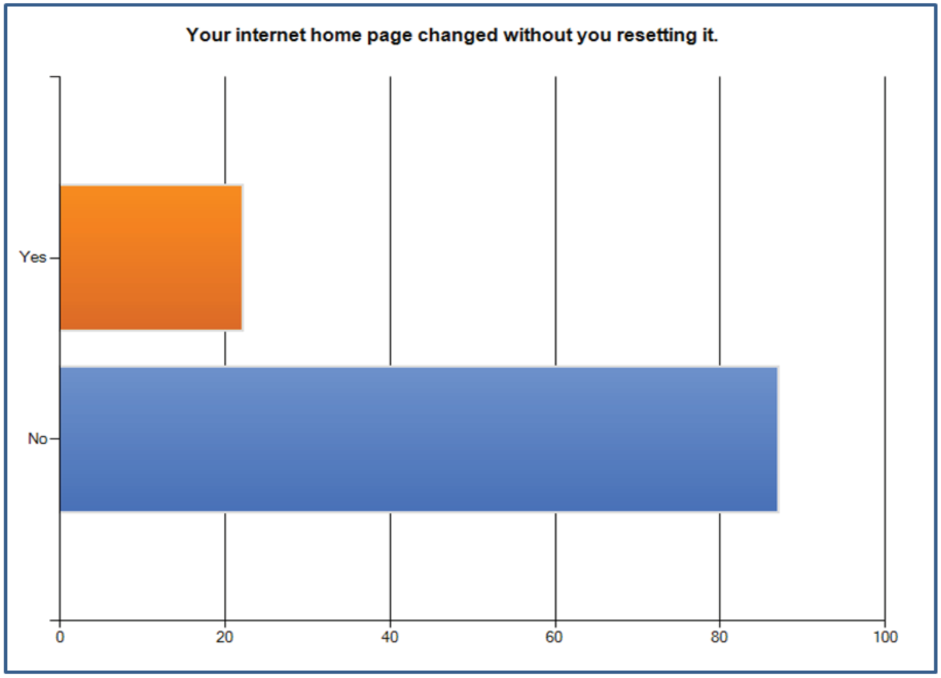


57 of the respondents have enjoyed are used to working diligently on their computer without experiencing any type of hardware glitches. The other 53 respondents that have answered yes, have all experienced their computer started freezing or it completely crashed or shuts down. Users have witnessed their keyboard locking up and their mouse freezing, leaving them with no other choice but to restart their system. These errors may be common and can be very frustrating, as unsaved work will be lost at the time the computer freezes. Viruses and spyware may cause a user's computer to freeze or crash.

Section 4.1, question 12 had 87 respondents answered no to this question. 1 respondent elected not to answer this question.

Table 12

Question 12: Your internet home page changed without you resetting it.

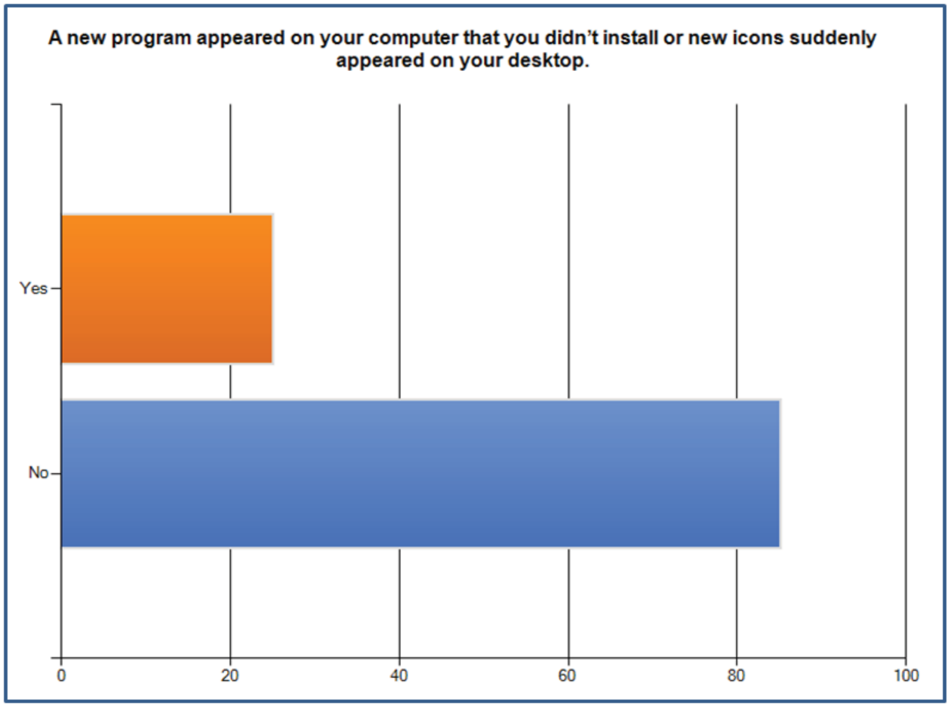


Internet browser hijacking is another type of online fraud. Browser hijacking may occur when a perpetrator is able to successfully exploit vulnerabilities in a user's browser application. Once the browser has been hijacked, the perpetrator is able to control how the browser operates. One example may include changing the default home page with the user resetting this. The chief concern is that browser settings may cause all of the traffic between the victim's browser and Internet websites to be routed through the perpetrators system. This will allow the perpetrator to follow the user's every move, and it may allow them to capture passwords you enter at sites such as online banking and financial institutions.

Section 4.1, question 13 had 85 respondents answered no to this question.

Table 13

Question 13: A new program appeared on your computer that you didn't install or new icons suddenly appeared on your desktop.

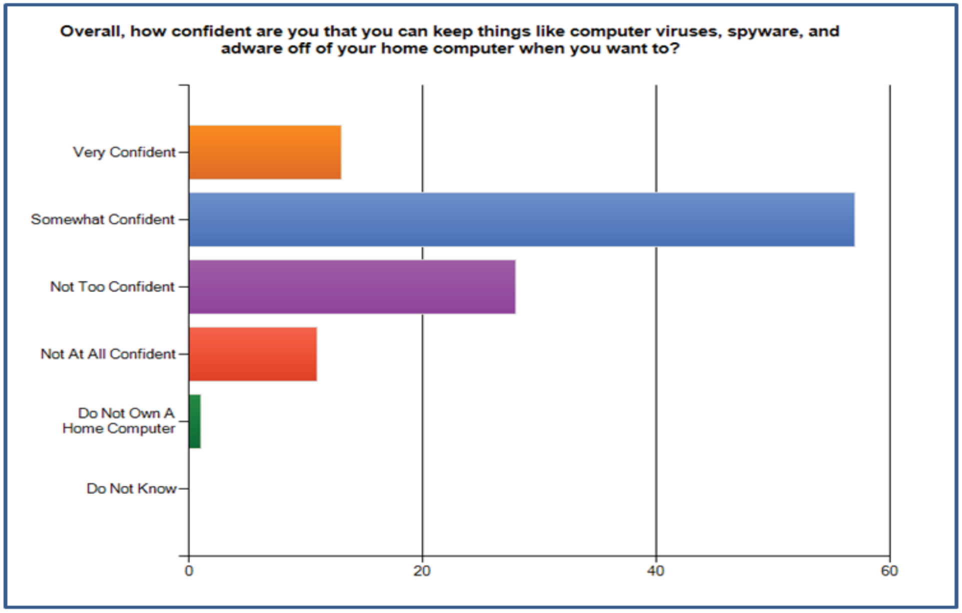


There are a number of ways spyware or other unwanted software can get installed on a user's computer. The most common form of unwanted software installations may come from a P2P file sharing programs. As a user downloads a P2P program to download music or video, unwanted applications may covertly install itself on the computer. Free software like weather programs, browser toolbars, and screen savers sometimes install spyware on a user's computer. During the installation, a license agreement will indicate that it is installing extra software is going to be installed. Many users' do not take the time to read license agreements and often do not realize the implications that this may cause. These freeware applications may collect information about the user's browsing habits and display advertisements tailored to their interests. Other malicious software may scan the hard drive of the user and capture their personal information, such as passwords and banking information. Once the information has been collected, this may transmitted to the perpetrator. In other cases, malicious applications may shut down your anti-spyware or anti-virus programs leaving a user's computer vulnerability.

Section 4.1, question 14 had 57 out of 110 respondents are somewhat confident that they can keep this malicious software off of their computers.

Table 14

Question 14: Overall, how confident are you that you can keep things like computer viruses, spyware, and adware off of your home computer when you want to?

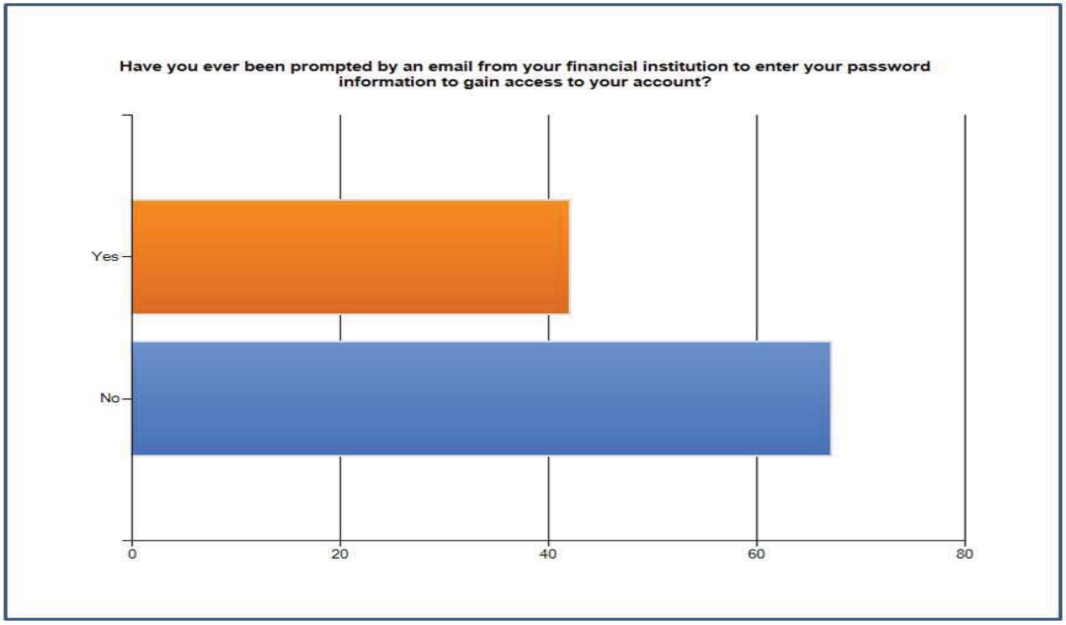


The reality of the situation is that most of the respondents will not be able to keep spyware, viruses, and adware off of their computers. As technology continue to advance and more users become more reliant on the Internet, keeping computers free of malware is becoming more of a daunting task. Software developers of spyware are becoming more cunning by developing web pages that installs spyware on a user's computer simply by visiting it. Even with anti-virus or anti-spyware programs, it has been documented that as many as 90% of U.S. home computers have been infected with spyware at some point in time. 20% of computers will be infected by viruses. 58% of the viruses are designed to steal bank card passwords and collect personal information. The large majority of users do not know how to resolve this common occurrence. P2P applications, such as LimeWire presents a major security risk to home users.

Section 4.1, question 15 had 67 out of 109 respondents answered no. 1 respondent elected not to answer this question.

Table 15

Question 15: Have you ever been prompted by an email from a financial institution to enter your password information to gain access to your account?

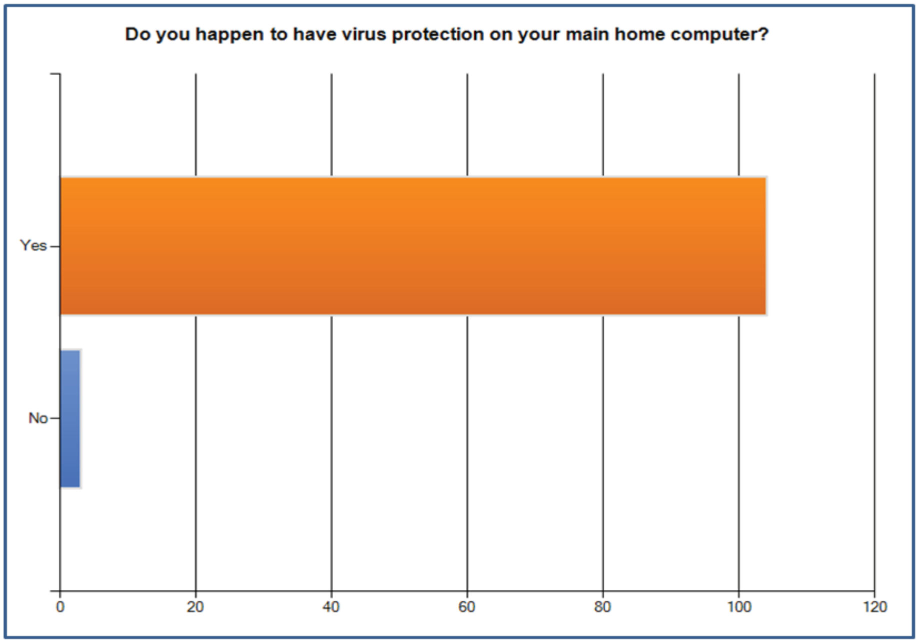


Perpetrators use phishing scams to entice users to giving up their account numbers, passwords, Social Security numbers and other confidential information that they will use to run up bills on credit cards or loot checking accounts. Banks or other financial institutions will never ask users for their confidential information through regular email. Furthermore, users will never be asked for their password or PIN numbers as well via email. Users should always proceed with caution if they are ever prompted for their account information. In the event users see any suspicious emails, it should be reported to the Federal Trade Commission.

Section 4.1, question 16 had 104 out of 107 respondents answered yes. 3 respondents elected not to answer this question.

Table 16

Question 16: Do you have virus protection on your main home computer?

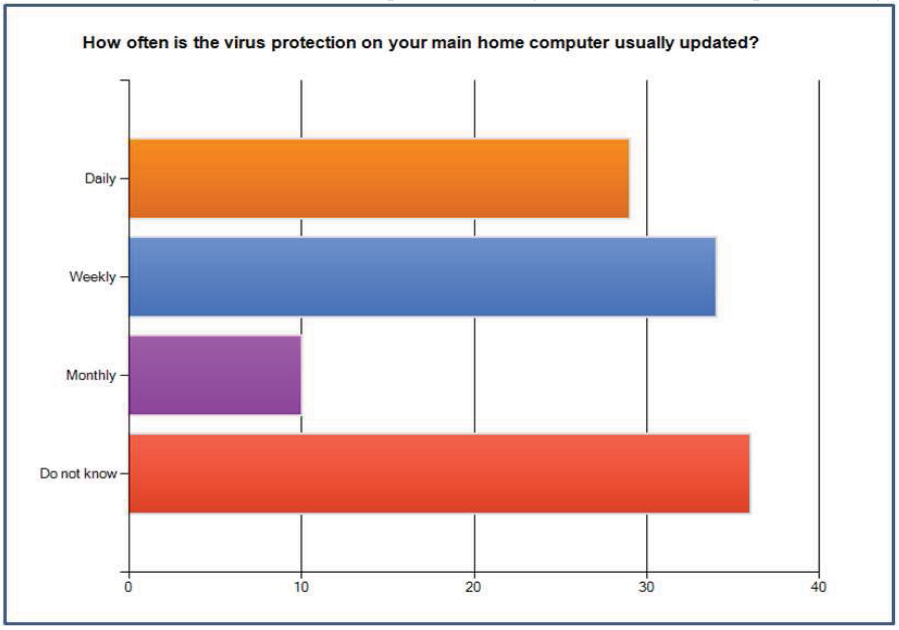


"Nevertheless 10 percent of Internet users do not use any virus protection and just as many only rely on risky On Demand scanners." (Rothbart, 2008) These days as more users pay their bills, store sensitive information, manage their financial accounts, and buy merchandise online; there should be more emphasis on keeping computers secure. Perpetrators are always discovering new vulnerabilities to exploit in computer software to gain control of user's computer and gain access to secure information. Users that have downloaded a virus onto their computers will always subjugate themselves to perpetrators watching users every action on their computer, or cause damage to the computer by reformatting a hard drive or changing data. Users also have to be mindful that they install a credible anti-virus application like Symantec or AVG as an example. Perpetrators are now using popup ads that may represent IT vendors offering to check user's computers for viruses. The pop up advertisement can sound so alarming because they are designed to get the users attention by convincing them to scan or clean their computer immediately with the offered tool. Victims will be misled into paying a cost to download fake security software, but the ultimate goal is to obtain credit card information.

Section 4.1, question 17 had 36 out of 109 respondents did not know how often their antivirus updated the virus definition file. This represents 33% of the total population. 1 respondent elected not to answer this question.

Table 17

Question 17: How often is the virus protection on your main home computer usually updated?

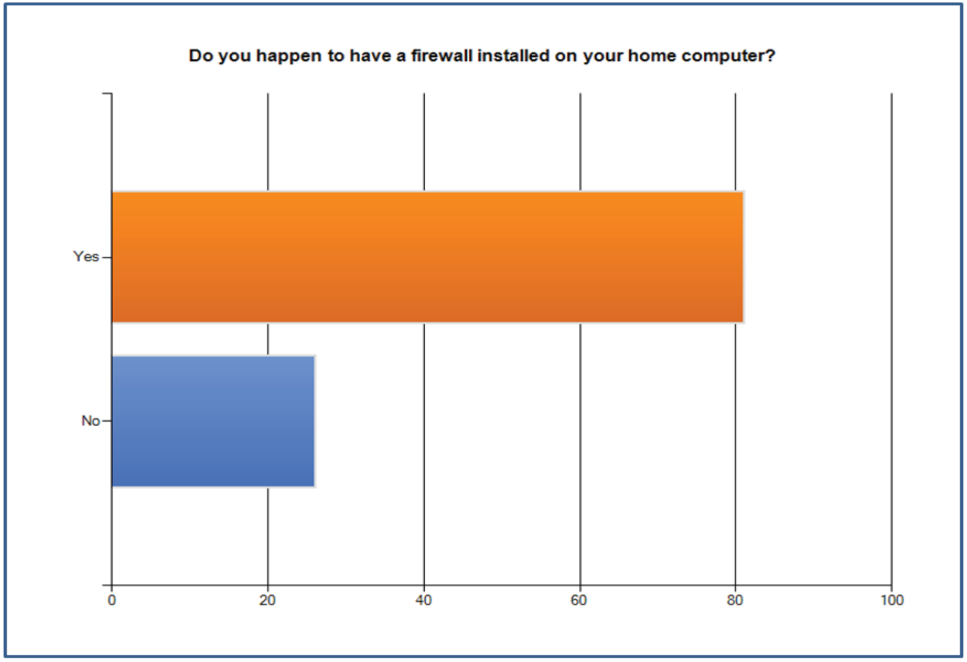


There are millions of different types of viruses that exist, with hundreds more being created and used daily. It may take anti-virus companies to develop and distribute a virus definition file a day, a week, or even longer to detect and quarantine the latest virus. The definition file contains a list of known viruses that the antivirus application uses when searching and quarantining viruses. When users neglect to update their computers, this will place them at risk for a number of computer crimes. Computers that have been infected by viruses will communicate and steal personal information. This information will then be transmitted to the perpetrator before the user even notices what happens. A general rule of thumb is to update your antivirus application weekly, if the internet is used occasionally (one hour per day or less). If users use the internet daily (one hour per day), antivirus applications should be updated daily. If users are on the internet for more than an hour per day, antivirus applications should be updated hourly.

Section 4.1, question 18 had 81 out of 107 respondents answered yes. This represents 75.7% of the total population. 3 respondents elected not to answer this question.

Table 18

Question 18: Do you happen have a firewall installed on your home computer?

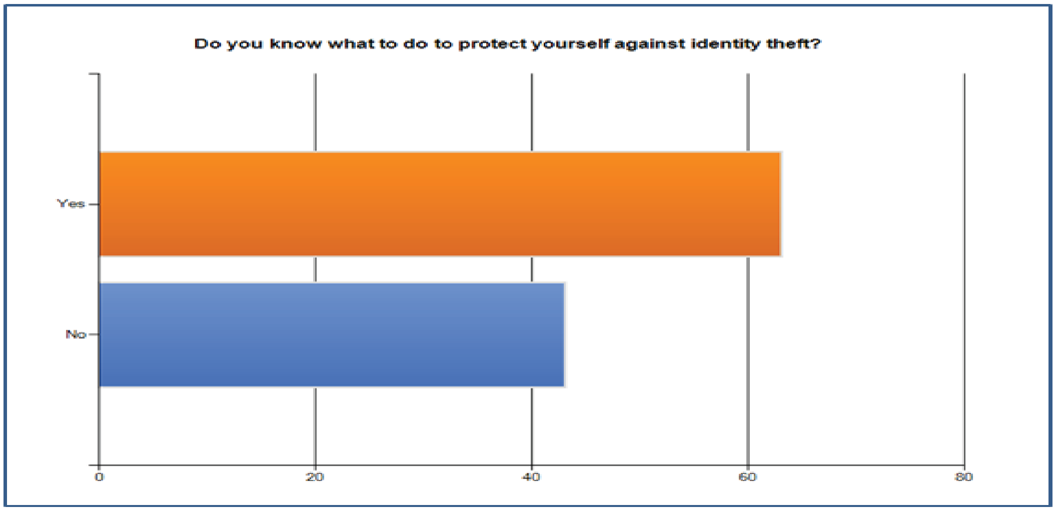


The internet makes it possible for viruses and spyware to communicate with perpetrators to steal personal information, control computers from remote locations, and install bad software. Perpetrators are targeting home computers to make money by stealing user's information. Firewalls serve as a barrier between a computer and the Internet. The purpose of a firewall is to guard user's computers from threats like viruses by filtering out any suspicious traffic that is sent. Just like caller ID on a telephone that identifies who is calling before answering the call; a firewall operates among the same lines. The firewall can identify who is trying to chat to the user's computer and discern whether or not to allow communication to come through. Firewalls can also be configured to prevent traffic from leaving user's computers and going out to the internet. This will become very useful while preventing spyware from sending out personal information without user consent. Today, users that use Mac and Windows operating systems have a software version of a firewall installed.

Section 4.1, question 19 had 63 out of 106 respondents answered yes. This represents 59.4% of the total population. 4 respondents elected to skip this question.

Table 19

Question 19: Do you know what to do to protect yourself against identity theft?



> Every four seconds, an identity theft is stolen in the U.S. Victims can spend years recovering from theft and attempting to clean up the mess it leaves behind, including lost job opportunities, refusal of loans for houses and cars and even jail time as a result of false data in law enforcement records. (Max, 2008)

When it comes to the crime of identity theft, there is no way of controlling whether or not users will become a victim. If personal information is deliberately stolen or accidently disclosed, taking certain steps quickly can mitigate the potential for the theft of identity. Victims should place a fraud alert on their credit reports and review the reports carefully. By placing the alert the creditor will have to follow certain guidelines before they open new accounts in the victim's name or make changes to your existing accounts. There are three nationwide consumer reporting companies that have toll-free numbers for placing a fraud alert within a 90 day timeline. Contacting one company should be sufficient enough where all consumer reporting companies will be notified:

- Equifax: www.equifax.com, 1-800-525-6285
- TransUnion: www.transunion.com, 1-800-680-7289
- Experian: www.experian.com, 1-888-EXPERIAN (397-3742)

By placing a fraud alert, the victim is entitled to free copies of their credit reports. Victims should look for inquiries from companies that they have not contacted, debts on their accounts that cannot be explained, and accounts that they did not open.

Close any accounts that have been established or tampered with fraudulently:

- Contact the fraud or security departments of each company where an account was changed or opened without the victims consent.
- Keep of copies of documents of conversation about the identity theft crime.
- Request documentation that the disputed account has been closed and the fraudulent debts discharged.

Victims should notify state agencies if their driver's license or government issued identification has become compromised. Contact the agency that issued the identification document or license. There will be procedures that should be followed when canceling documents and trying to get a replacement. Victims should request that the agency flag their file so that perpetrators cannot get a license or any other identification documentation from them in the victim's name.

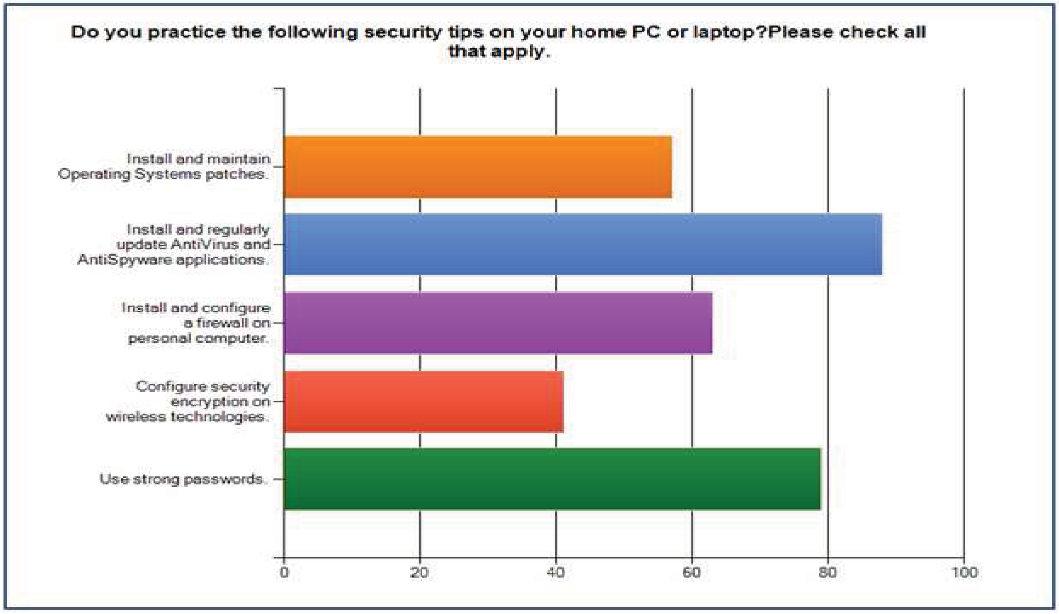
Victims should look to file a police report, then get the number of the report or request a copy of the police report. This will help with dealing with creditors who may request proof of the identity theft crime. Police officers that may be reluctant to take a report, victims may ask to file with another jurisdiction, like the state police, or request to file a miscellaneous incidents report. As a last resort victim's can check with their state Attorney General office to find out if state law requires the police to take reports for identity theft. Victims should also report identity theft to the Federal Trade Commission. This report will help law enforcement officials across the country in their investigations.

Online: www.ftc.gov/complaint
Phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261

Section 4.1, question 20 had 88 out of 101 respondents chose, "install and regularly update Antivirus and AntiSpyware applications" as the primary security function. This represents 87.1% of the total population. 9 respondents elected not to answer this question.

Table 20

Question 20: Do you practice the following security tips on your home PC or laptop? Please check all that apply.



The most successful way to protect a computer is to employ a layered security approach. Users should not expect one method to solve all of their problems, so multiple methods should be used to deal with different weaknesses. Each layer of security is different and even if perpetrators manage to penetrate one layer, the same techniques cannot be used to penetrate other layers. Granted, the only way to 100% secure a computer is to disconnect the computer from the internet and power it off. This will make the computer useless to any identity thief.

Today, Windows is the most frequently used operating found on personal computers today. Since there are more potential targets, security exploits are designed and carried out against computers running Windows. For perpetrators, Windows is where the money is. Users that are still using Windows 95, 98 and ME operating systems, there is no security. It would be best to purchase a new computer that has Windows 7 installed. With all of the new vulnerabilities and security holes that continue to be found, users should always take it upon themselves to update their operating system. This will also apply to internet browsers and applications. Windows updates can be set to run automatically or manually.

A good antivirus and antispyware application, properly updated and configured is a must. Computers can easily be infected with viruses, spyware, and pop-ups. The types of malicious malware that users encounter are seemingly endless. The amount of effort to find and provide fixes for spyware and viruses is astonishing. Malicious software is getting more complicated and the number of them continues to increase. Viruses are becoming more effective in that they propagate themselves quickly and they often hide themselves and are intelligent enough to move around in a system by renaming itself in an effort to make it difficult to remove them. Nowadays, antivirus and antispyware applications come bundled together. User's should become familiar with the applications real-time scan feature and configure it to start automatically each time the computer has been powered on. Some of the recommended reputable companies that are out on the market today are the following: AVG, Symantec, and Panda.

The internet has a wealth of information that is readily available to the average computer user at home, in education, and in business. For many users it is essential that they have access to this information. Users that use their computer to connect to the internet can expose confidential or critical information to malicious attacks. Firewall protects users from anything that might get through the other layers of defense. A firewall can be likened to a valve that user's access the internet, but prevents the internet from accessing the user. The purpose of a firewall is to mask information and activity from the internet. Firewall applications may protect user's computers from hostile intrusions by alerting them when a perpetrator tries to access their computers.

Wireless home networks have exploded onto the scene within the last few years, which was driven by inexpensive equipment and the desire to set up home networks quickly. However, many users did not realize that they were exposed to a significant amount of security risks. Wireless networks are often configured by default to allow access to any computer that attempts to connect to the network. Wireless networks are setup pretty easily, and users often do not realize that they are offering free bandwidth to anyone who chooses to use it. Users may be exposing their home network to illegal activity, such as spamming. In order to protect user's their data from snooping or prying eyes, wireless networks should be encrypted, so that perpetrators cannot read it. Most recent wireless equipment comes with both WEP (wired equivalent privacy) and WPA (wifi protected access) encryption methods that may be enabled. WEP is considered the first generation of wireless networking encryption methods. This is considered to be the not the best form of security because it was fairly easy to crack. WPA was later rolled out to provide stronger wireless data encryption methods. In order to use WPA, all of the devices that are communicating on the network need to be configured for WPA.

A good password should have the ability to balance security with the ability with user's remembering it. The most interesting passwords are the easiest to crack, while the most secure are a hodgepodge of characters are impossible to remember. Passwords should be used at all sensitive points, such as the following: financial, email, and administrative accounts. While making a password, it should have a minimum of 8 characters and make it so others will have a hard time guessing it. Do not use words out of the dictionary, because perpetrators can use brute force attacks to crack the password. Passwords that may have been considered a strong password a few years ago may now be an open invitation to user's computers. Never use the same password for social networking, banking, and shopping accounts. If a perpetrator steals a victim's password that is the same for all of their accounts, they may impersonate them in online transactions or open new credit card accounts.

Chapter 5 – Conclusions

"Identity theft is considered to be one of the most pervasive forms of white-collar crime in the United States." (Rusch, 2010) One of the most common fraud schemes were when victims were contacted directly by criminals who used deception and lies to persuade the victims to part with their money. Today, identity theft requires no direct communication between the victim and the criminal. Phishing and spyware may give identity thieves enough of an opportunity to unauthorized access to personal information and commit identity theft.

Information has been provided showing not only what identity theft is and how it may occur, but also how users can do their part in preventing it and knowing what to do when they are affected. The harsh reality remains that no matter how many security measures that are implemented by users, there is no absolute way to prevent it. Even if the user has done everything possible to properly secure their computer, the threat still exists and always will. There are many perpetrators around who can electronically invade personal computers for personal information.

Identity theft continues to be a major problem that cannot be solved by financial companies alone. The industry needs to collaborate with other businesses, government, and the public. Financial companies should make themselves aware of proposed and existing legislation, both state and federal in relation to identity theft. The Federal Department of Justice is taking identity theft related crimes very seriously. Federal prosecutors around the country will continue to use criminal statues, and work closely with the FTC and other agencies, to fight this effectively. Most importantly, financial companies should work with the public to increase their awareness of identity theft issues. When the public becomes better educated about the subject of identity theft, they can become a great asset. Informing the public about identity theft problems can also help the consumers to be more prepared if they become a victim.

Statistics have shown that identity continue to climb on an annual basis. The current environment in which identity theft crimes advanced took years to develop, and it will take years to carry out effective means of preventing identity theft. Identity thieves are smarter than ever and are coming up with new and even more dangerous ways to uncover confidential data from unsuspecting victims. A collaborative effort by government, law enforcement, businesses, and the public is needed to curb its growth and reduce the incidence of identity theft. It is imperative that the public stay on top of their personal information. By making themselves aware of the existing scams, consumers can protect themselves more effectively because they know what dangers exist. Chances are if the readers of this thesis follow the suggested tips that are provided; the chances to falling victim of identity theft will reduce significantly.

References

Rather, Paul (2010). Identity Theft and Fraud – Here's Some Key Statistics You Need to Know! http://ezinearticles.com/?Identity-Theft-and-Fraud---Heres-Some-Key-Statistics-You-Need-to-Know!&id=2021315

Newman, John Q. (1999) Identity Theft: The Cybercrime of the Millenium. Pages (1) Port Townsend, WA: Loompanics Unlimited.

Vacca, John R. (2003) Identity Theft. Pages (4) New Jersey: Pearson Education, Inc.

Gerdes, Louise I. (2009) Cyber Crime. Pages (22, 25) Farmington Hills, MI: Greenhaven Press.

Stein, Richard Joseph. (2009). Internet Safety. Pages (67) New York: H.W. Wilson Company Intelligent Security Solutions. (2009) http://www.3ciss.com/New%20layout/phishing.html

McCall, Tom. Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks. December 2007. http://www.gartner.com/it/page.jsp?id=565125

Vicario, Marissa. The MessageLabs Intelligence Annual Security Report: 2009 Security Year in Review. 8 December 2009. http://www.symantec.com/connect/blogs/messagelabs-intelligence-annual-security-report-2009-security-year-review

How to Avoid Phishing. 2010. http://www.identityguard.com/how-to-avoid-phishing.aspx Mills, Elinor. A flood of phishing sites and how to avoid them. 10 September 2010. http://news.cnet.com/8301-27080_3-20016026-245.html

Sullivan, Bob Cell Phone Hacking Has Unlikely Ring. 22 June 2007. http://redtape.msnbc.com/2007/06/just-how-easy-i.html

Ciampa, Mark. (2005) Security+ Guide To Network Security Fundamentals. Pages(48) Boston, MA: THOMSON Course Technology.

Mitchell, Bradley. Keylogger. 2010. http://compnetworking.about.com/od/networksecurityprivacy/g/keylogger.htm

Keylogger. 10 March 2009. http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci962518,00.html

War Driving. 28 March 2002. http://searchmobilecomputing.techtarget.com/definition/war-driving

Synovate. Federal Trade Commission-Identity Theft Survey Report. 3 September 2003. http://www.ftc.gov/os/2003/09/synovatereport.pdf

Identity Theft Statistics 2010. 18 February 2010. http://www.identitytheftlabs.com/identity-theft/identity-theft-statistics-2010/

Official Identity Theft Statistics. 2009. http://www.spendonlife.com/guide/identity-theft-statistics

Ingram, Mathew. Identity Theft on the Rise: Survey. 10 February 2010. http://gigaom.com/2010/02/10/identity-theft-on-the-rise-survey/

2009 Identity Theft Statistics. 2009. http://www.spendonlife.com/guide/2009-identity-theft-statistics

Finklea, Kristin M. Identity Theft: Trends and Issues. 5 January 2010. http://www.fas.org/sgp/crs/misc/R40599.pdf

2009 Identity Theft Statistics. 2009. http://www.spendonlife.com/guide/2009-identity-theft-statistics

Consumer Sentinel Network Data Book for January – December 2009. February 2010. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf

Hwang, Kaiser. Identity Theft Soars for Twentysomethings. 3 March 2009. http://www.switched.com/2009/03/03/identity-theft-soars-for-twentysomethings/

Crime Victimization in the United States: Statistical Overviews. 2010. http://ovc.ncjrs.gov/ncvrw2010/pdf/6_StatisticalOverviews.pdf

Hunter, Jessica. Identity Theft Statistics: Information You Must Know. http://www.identitytheftfixes.com/identity_theft_statistics_information_you_must_know.html

DeJarnette, Willie. General Identity Theft Statistics Revealed. 2009. http://www.articlesnatch.com/Article/General-Identity-Theft-Statistics-Revealed/201053

Study: ITRC Encouraged by 2009 Victim Aftermath Study. 21 May 2010. http://www.databreaches.net/?p=11736

Frayer, Amanda. Fact Sheet about ID Theft. 4 January 2009. http://www.defendyourdollars.org/2009/01/factsheet_about.html

Internet World Stats Usage and Population Statistics. 2010. http://www.internetworldstats.com/top20.htm

Rothbart, Elisabeth. Avira survey: Ten percent of internet users still surf unprotected. 8 July 2008. http://row.avira.com/ko/company_news/internet_users_surf_unprotected.html

The Identity Theft And Assumption Deterrence Act. 2008. http://www.identity-theft-tips.com/the-identity-theft-and-assumption-deterrence-act/

Kitten, Tracy. A Phishing Scam Compromised His Account, Changed His Life. 25 October 2010. http://www.bankinfosecurity.com/podcasts.php?podcastID=805

10 Unbelievable Yet True Identity Theft Stories. October 2007. http://identity-theft-solution.org/uncategorized/10-unbelievable-yet-true-identity-theft-stories

Handschuch, Dawn. Preventing Identity Theft: Swiping and Skimming – All in a Day's Work? 2009. http://www.creditfyi.com/Identity-Theft/Identity-Theft-Stories/Skimming,-Swiping-as-Credit-Card-Fraud.htm

Senator Maria Cantwell: Fighting Identity Theft. http://cantwell.senate.gov/issues/ID/stories.cfm

Identity Theft and Password Security chart. 7 June 2010. http://www.symantec.com/connect/blogs/identity-theft-and-password-security-chart

Siciliano, Robert. Social Media and Identity Theft Risks PT II. 30 March March 2010. https://www.infosecisland.com/blogview/3456-Social-Media-and-Identity-Theft-Risks-PT-II.html

Spyware/Privacy Warning Signs. 2010. http://www.worldstart.com/tips/tips.php/1344

Hayes, Eric J. Playing it Safe: Avoiding Online Gaming Risks. 2008. http://www.us-cert.gov/reading_room/gaming.pdf

Max. Identity Theft – Phishing: EDS' Eight Tips for Consumers to Protect Themselves from Identity Theft. 8 August 2008. http://www.bestsecuritytips.com/news+article.storyid+624.htm

Rusch, Jonathan J. Identity Theft: The Scope of the Problem. March 2008. http://www.youreviltwin.net/identity-theft-scope-of-problem.html

Antivirus Program. 2010. http://www.webopedia.com/TERM/A/antivirus_program.html

Browser Hijacker. 2010. http://www.webopedia.com/TERM/B/browser_hijacker.html

PDA. 2010. http://www.webopedia.com/TERM/P/PDA.html

Spyware. 2010. http://www.webopedia.com/TERM/S/spyware.html

Virus. 2010. http://www.webopedia.com/TERM/V/virus.html

Trojan Horse. 2010. http://www.webopedia.com/TERM/T/Trojan_horse.html

Wardriving. 2010. http://www.webopedia.com/TERM/W/wardriving.html

WEP. 2010. http://www.webopedia.com/TERM/W/WEP.html

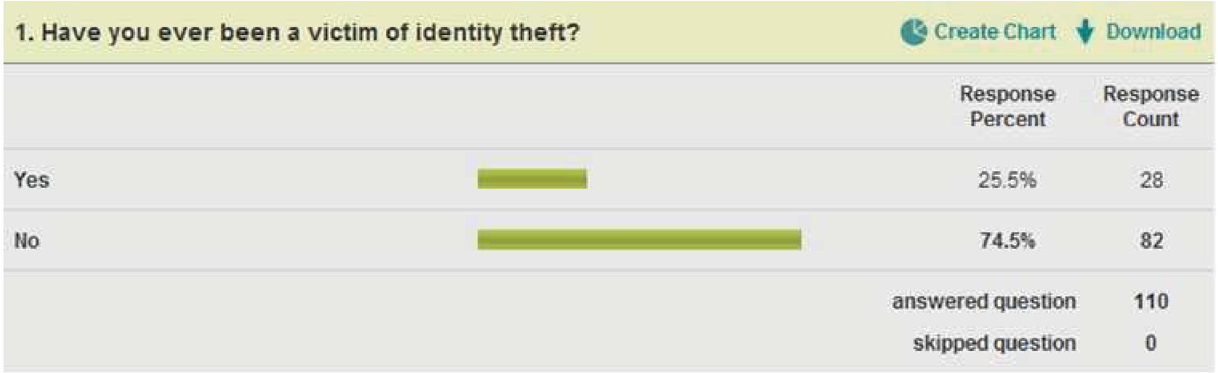
P2P (Peer To Peer). 2010. http://www.techterms.com/definition/p2p

WPA. 2010. http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3DWPA&i%3D54879%2C00.asp

Appendix A

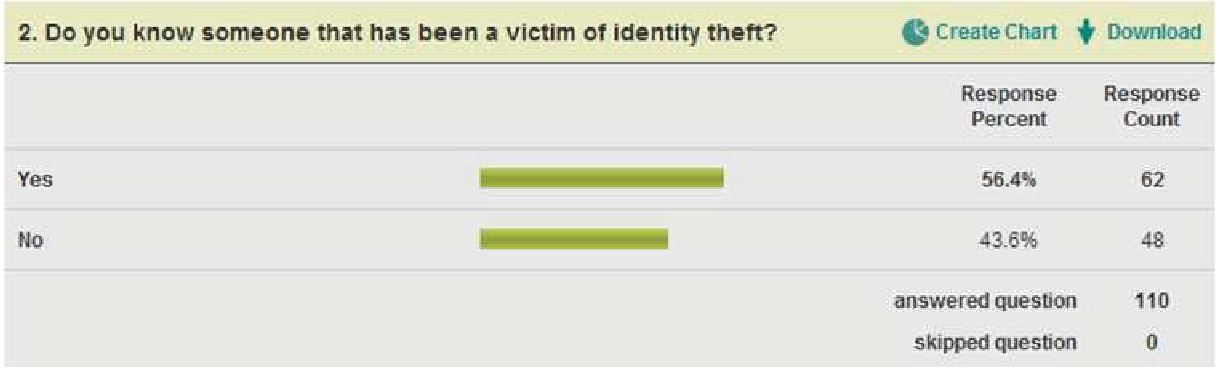
Table 2

Responses to Merrick & Company survey



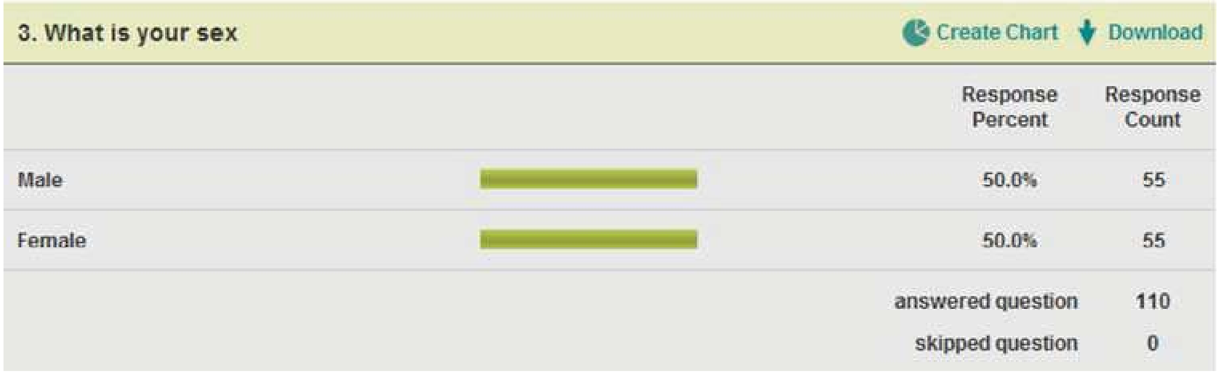
1. Have you ever been a victim of identity theft?

	Response Percent	Response Count
Yes	25.5%	28
No	74.5%	82
answered question		110
skipped question		0



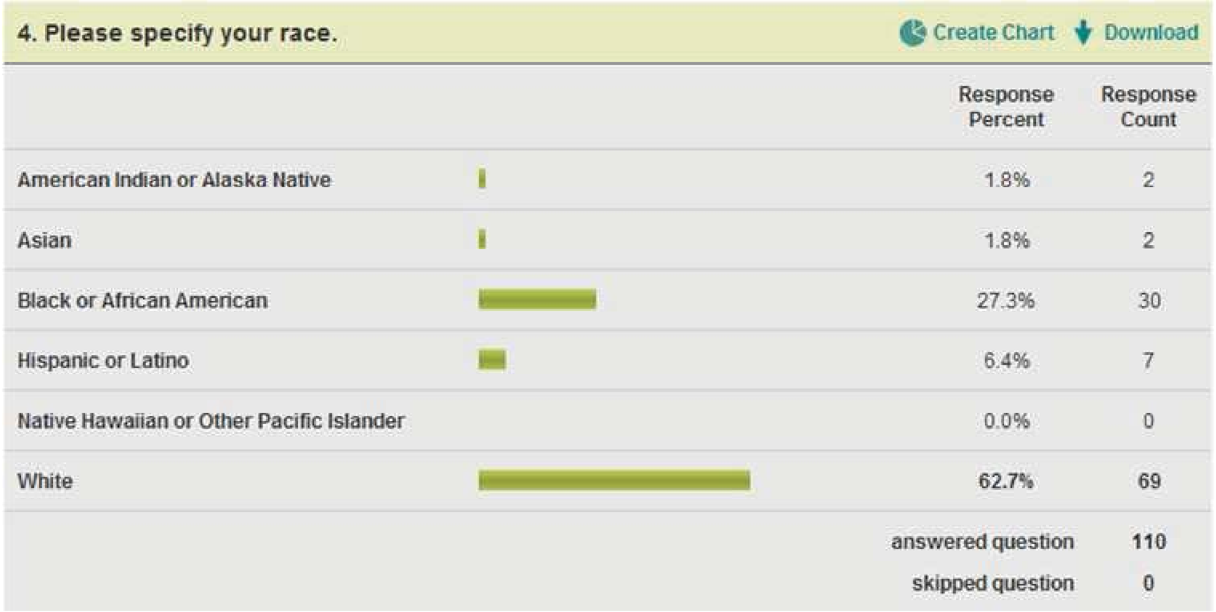
2. Do you know someone that has been a victim of identity theft?

	Response Percent	Response Count
Yes	56.4%	62
No	43.6%	48
answered question		110
skipped question		0



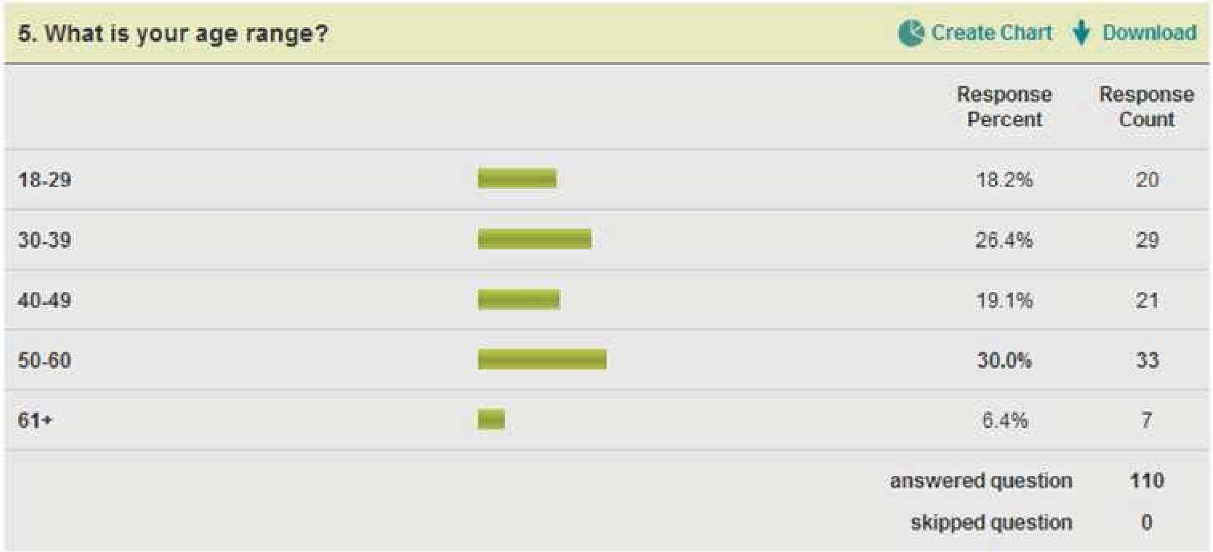
3. What is your sex

	Response Percent	Response Count
Male	50.0%	55
Female	50.0%	55
answered question		110
skipped question		0



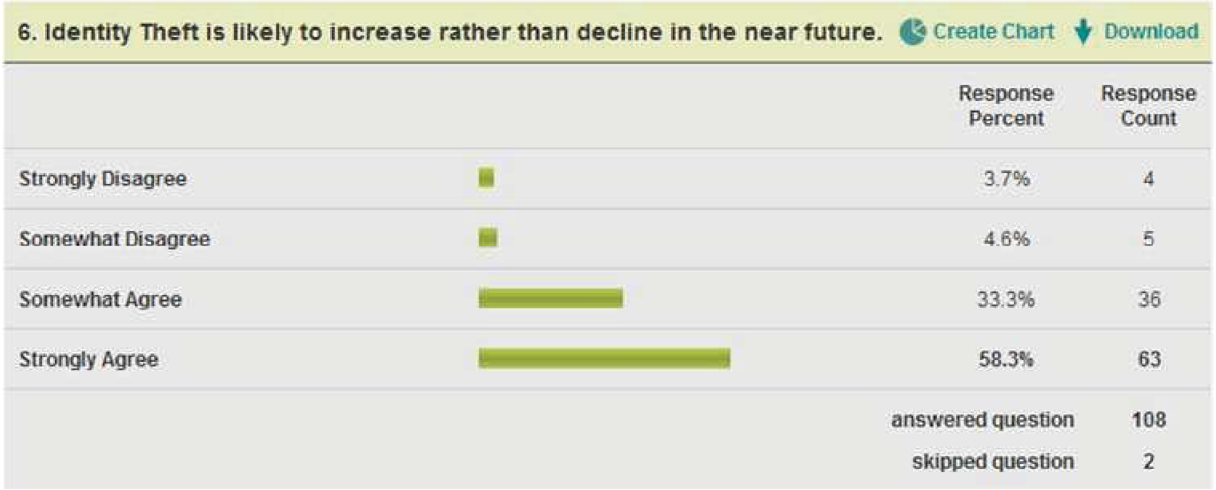
4. Please specify your race.

	Response Percent	Response Count
American Indian or Alaska Native	1.8%	2
Asian	1.8%	2
Black or African American	27.3%	30
Hispanic or Latino	6.4%	7
Native Hawaiian or Other Pacific Islander	0.0%	0
White	**62.7%**	**69**
	answered question	**110**
	skipped question	**0**



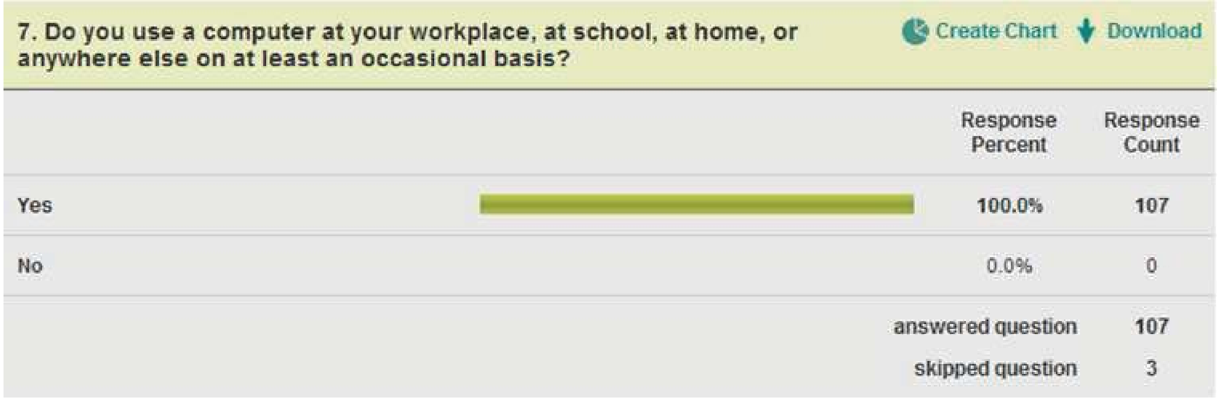
5. What is your age range?

	Response Percent	Response Count
18-29	18.2%	20
30-39	26.4%	29
40-49	19.1%	21
50-60	**30.0%**	**33**
61+	6.4%	7
	answered question	**110**
	skipped question	**0**



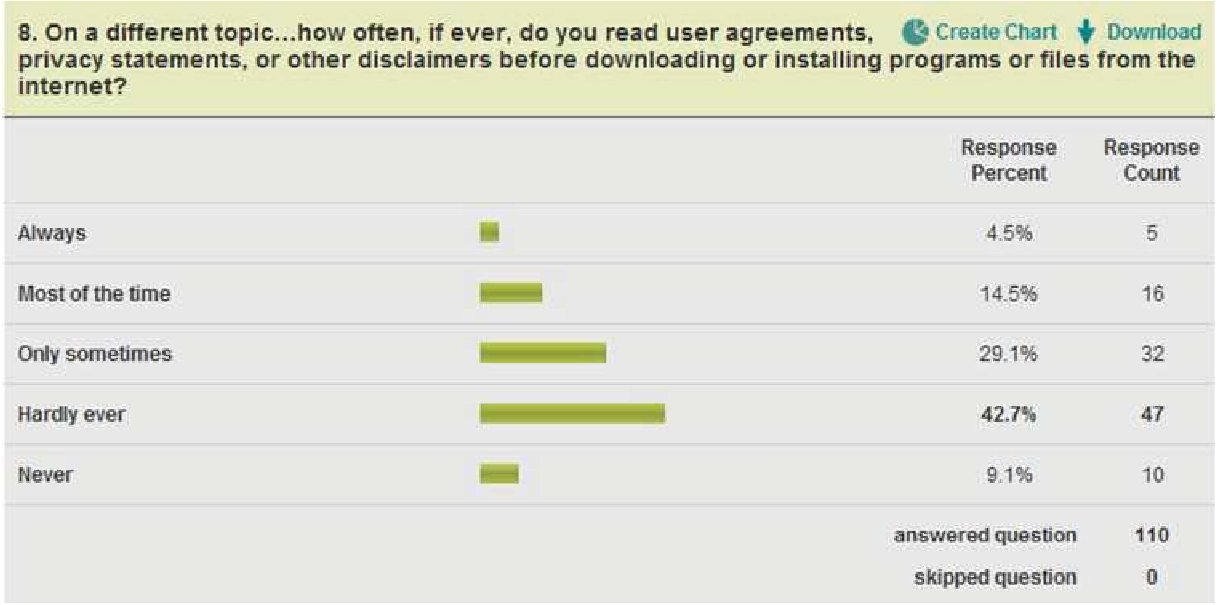
6. Identity Theft is likely to increase rather than decline in the near future.

	Response Percent	Response Count
Strongly Disagree	3.7%	4
Somewhat Disagree	4.6%	5
Somewhat Agree	33.3%	36
Strongly Agree	58.3%	63
answered question		108
skipped question		2



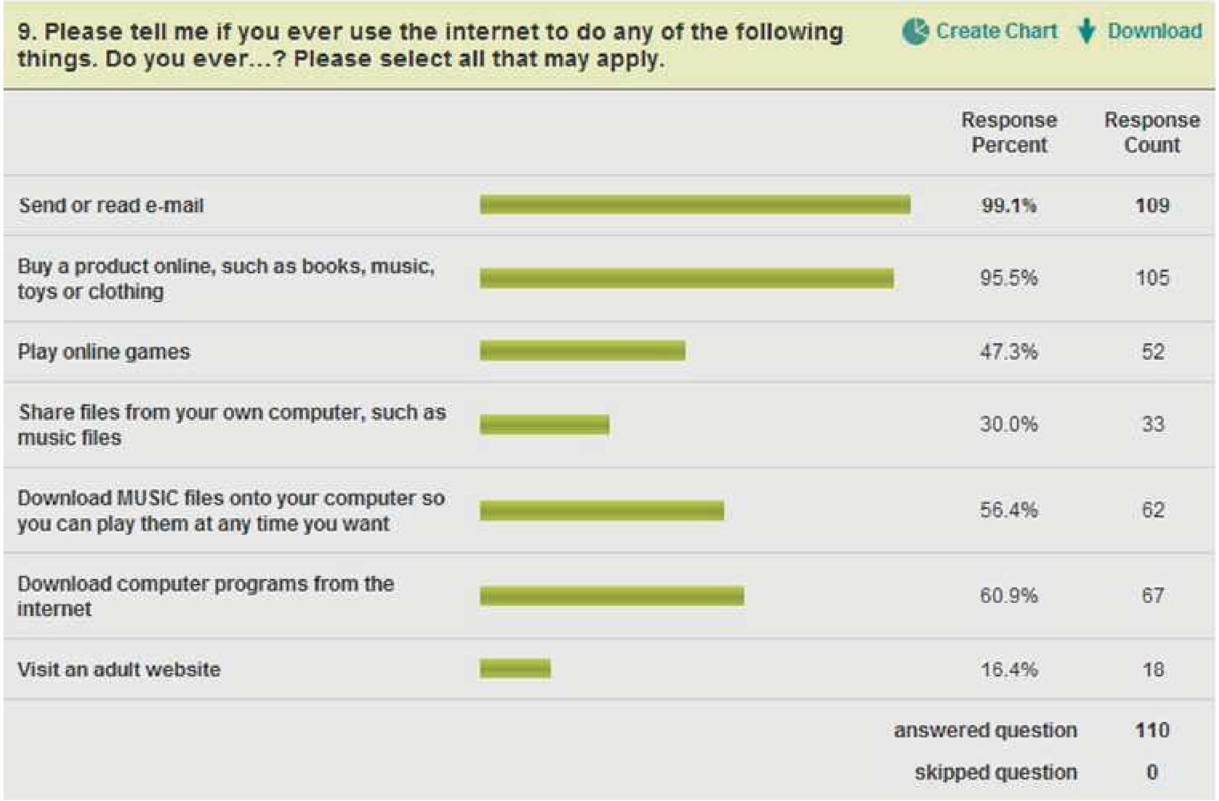
7. Do you use a computer at your workplace, at school, at home, or anywhere else on at least an occasional basis?

	Response Percent	Response Count
Yes	100.0%	107
No	0.0%	0
answered question		107
skipped question		3



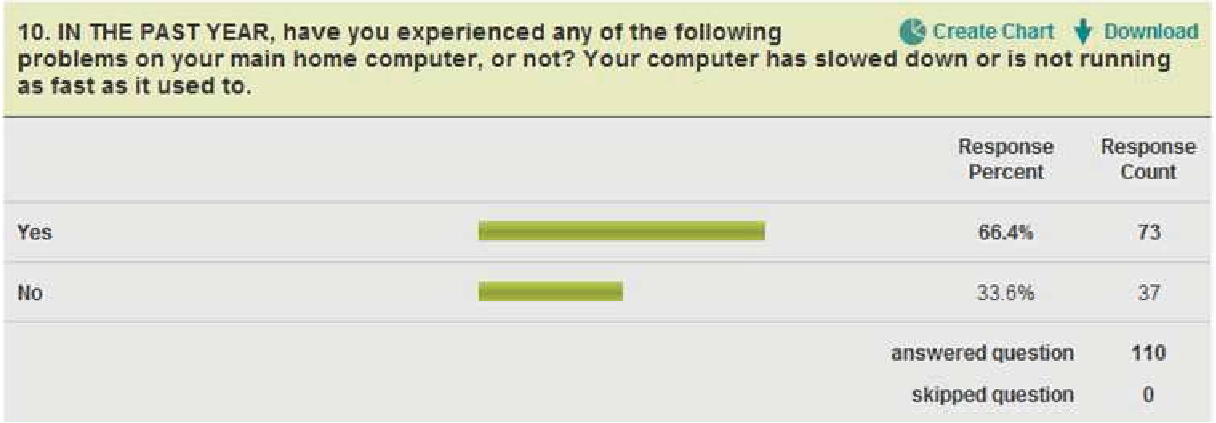
8. On a different topic...how often, if ever, do you read user agreements, privacy statements, or other disclaimers before downloading or installing programs or files from the internet?

	Response Percent	Response Count
Always	4.5%	5
Most of the time	14.5%	16
Only sometimes	29.1%	32
Hardly ever	42.7%	47
Never	9.1%	10
answered question		110
skipped question		0



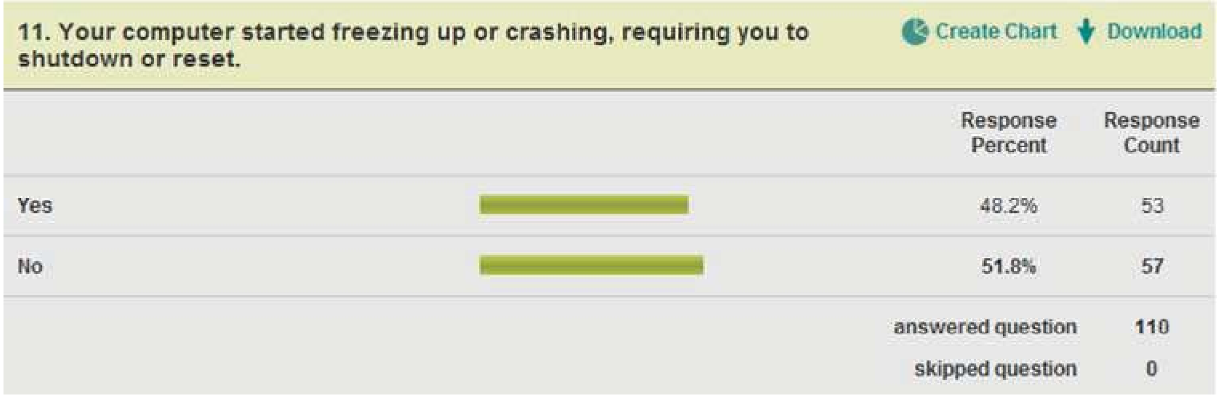
9. Please tell me if you ever use the internet to do any of the following things. Do you ever...? Please select all that may apply.

	Response Percent	Response Count
Send or read e-mail	**99.1%**	**109**
Buy a product online, such as books, music, toys or clothing	95.5%	105
Play online games	47.3%	52
Share files from your own computer, such as music files	30.0%	33
Download MUSIC files onto your computer so you can play them at any time you want	56.4%	62
Download computer programs from the internet	60.9%	67
Visit an adult website	16.4%	18
	answered question	110
	skipped question	0



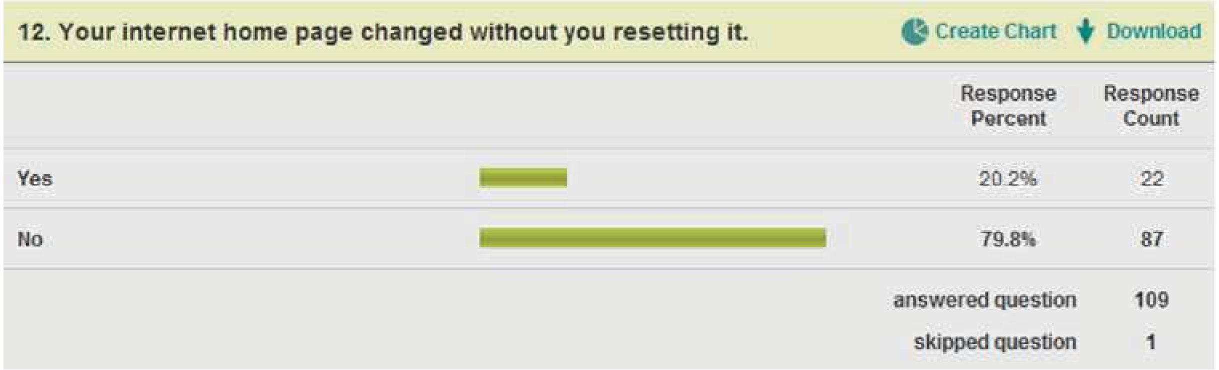
10. IN THE PAST YEAR, have you experienced any of the following problems on your main home computer, or not? Your computer has slowed down or is not running as fast as it used to.

	Response Percent	Response Count
Yes	**66.4%**	73
No	33.6%	37
	answered question	110
	skipped question	0



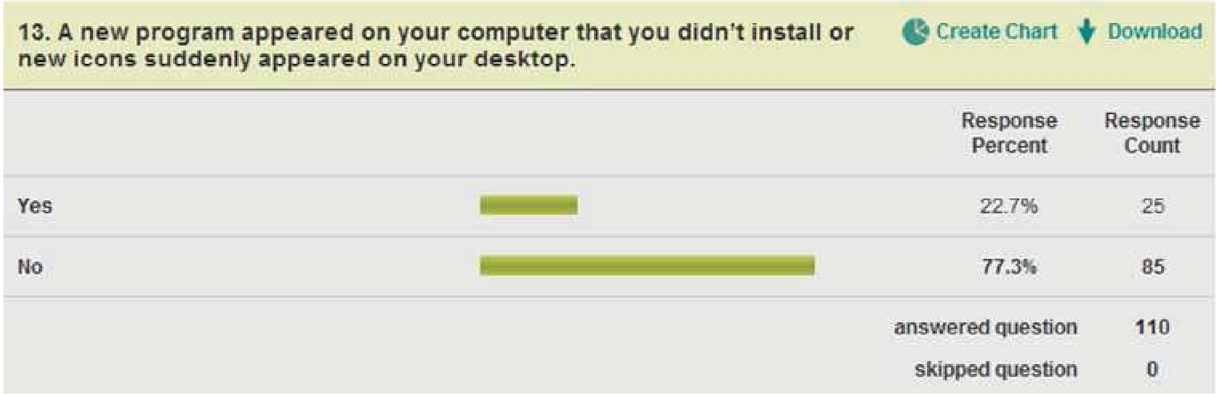
11. Your computer started freezing up or crashing, requiring you to shutdown or reset.

	Response Percent	Response Count
Yes	48.2%	53
No	51.8%	57
answered question		110
skipped question		0



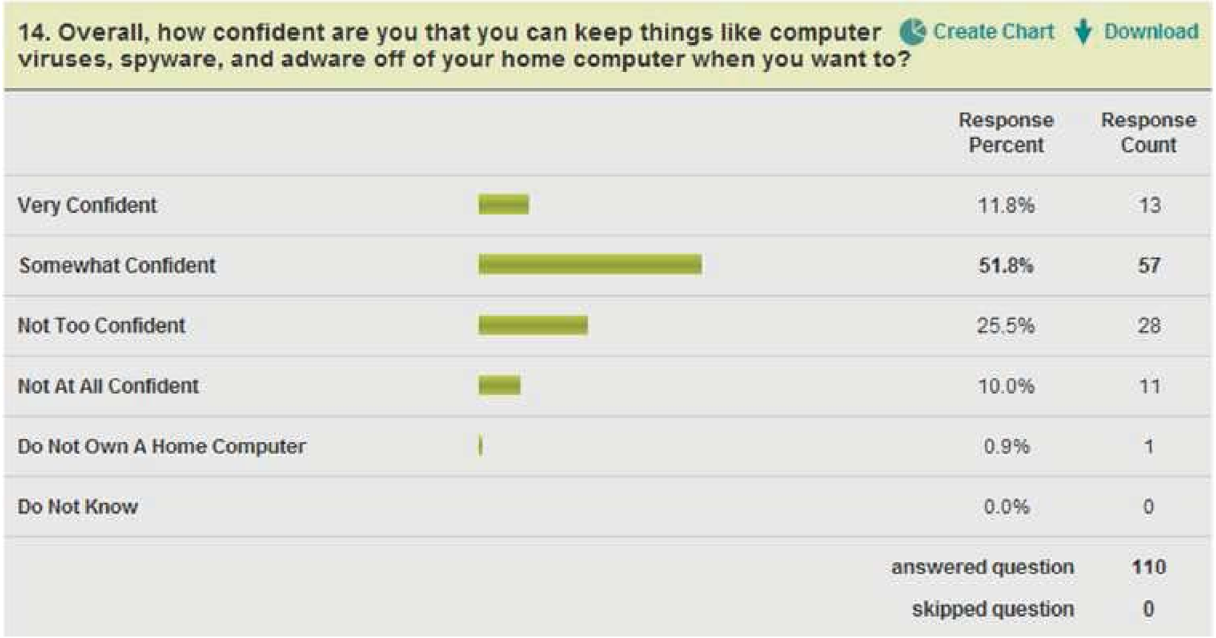
12. Your internet home page changed without you resetting it.

	Response Percent	Response Count
Yes	20.2%	22
No	79.8%	87
answered question		109
skipped question		1



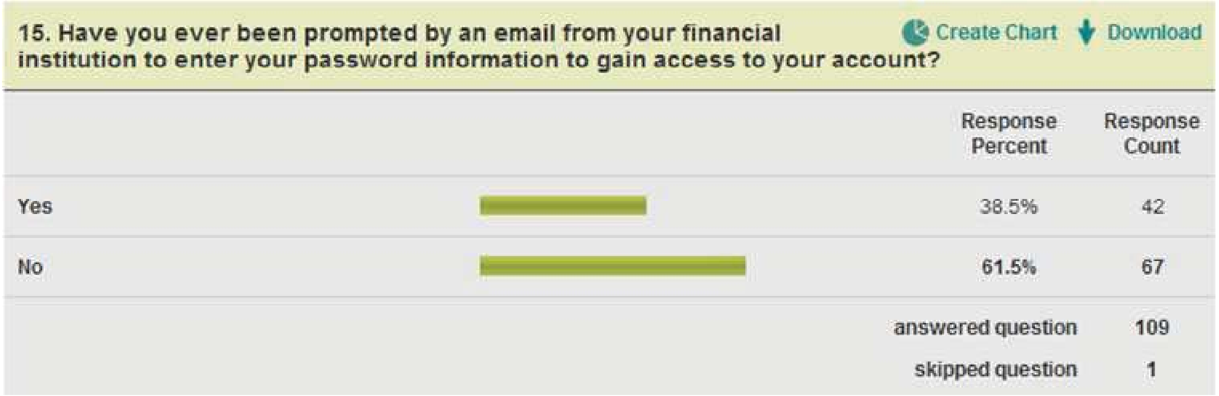
13. A new program appeared on your computer that you didn't install or new icons suddenly appeared on your desktop.

	Response Percent	Response Count
Yes	22.7%	25
No	77.3%	85
answered question		110
skipped question		0



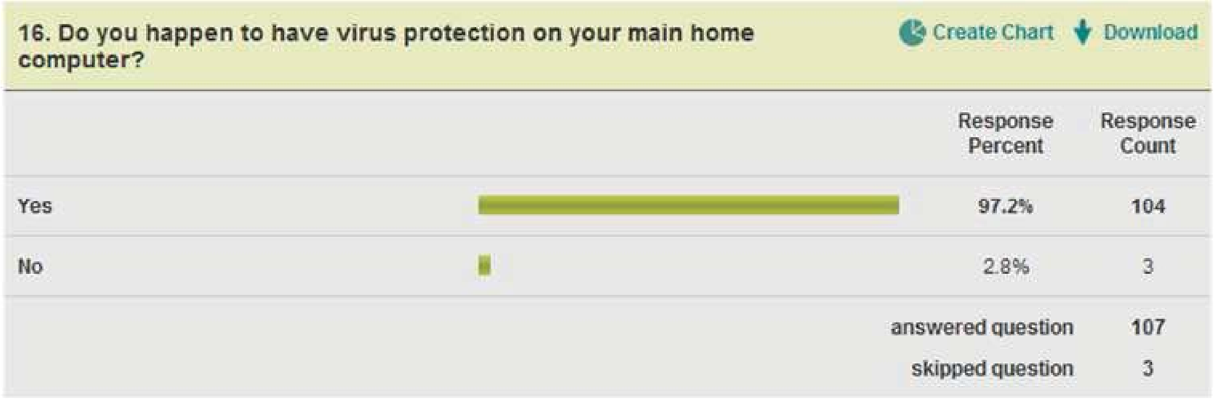
14. Overall, how confident are you that you can keep things like computer viruses, spyware, and adware off of your home computer when you want to?

	Response Percent	Response Count
Very Confident	11.8%	13
Somewhat Confident	**51.8%**	**57**
Not Too Confident	25.5%	28
Not At All Confident	10.0%	11
Do Not Own A Home Computer	0.9%	1
Do Not Know	0.0%	0
	answered question	**110**
	skipped question	**0**



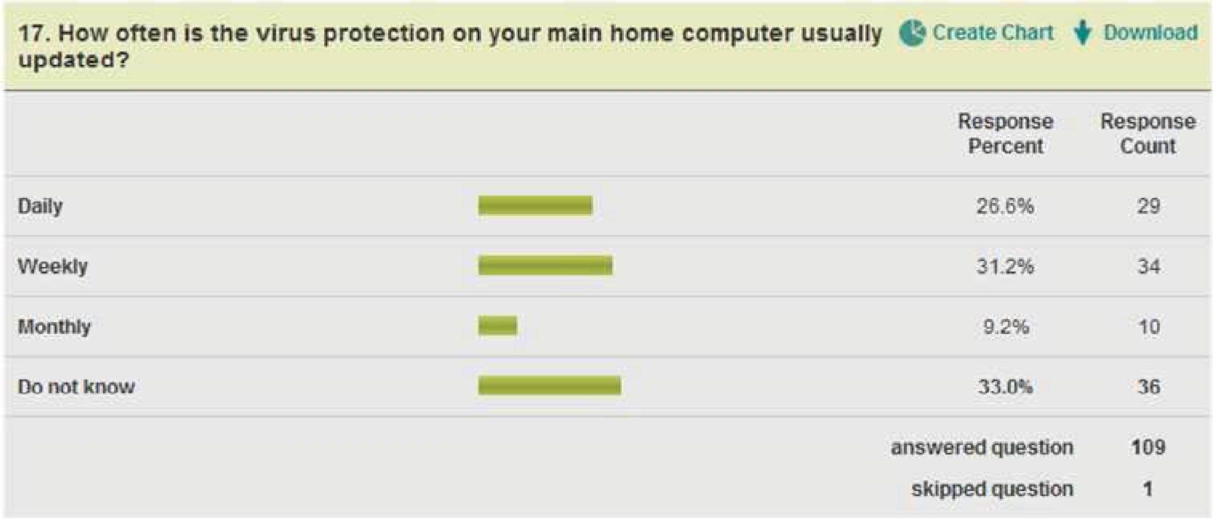
15. Have you ever been prompted by an email from your financial institution to enter your password information to gain access to your account?

	Response Percent	Response Count
Yes	38.5%	42
No	**61.5%**	**67**
	answered question	**109**
	skipped question	**1**



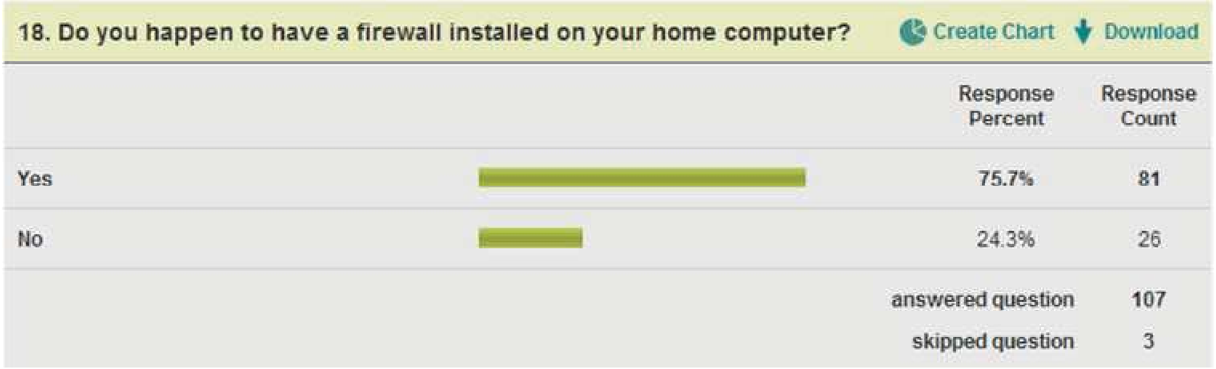
16. Do you happen to have virus protection on your main home computer?

	Response Percent	Response Count
Yes	**97.2%**	**104**
No	2.8%	3
	answered question	**107**
	skipped question	**3**



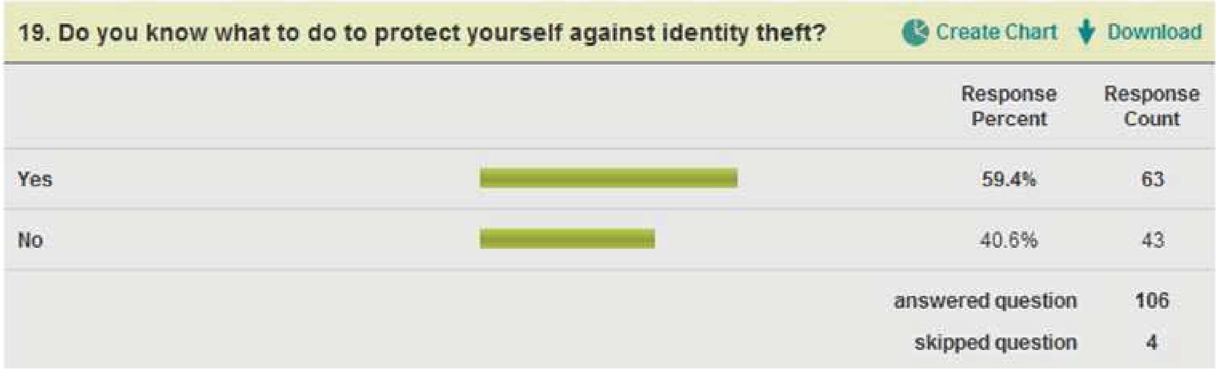
17. How often is the virus protection on your main home computer usually updated?

	Response Percent	Response Count
Daily	26.6%	29
Weekly	31.2%	34
Monthly	9.2%	10
Do not know	33.0%	36
	answered question	109
	skipped question	1



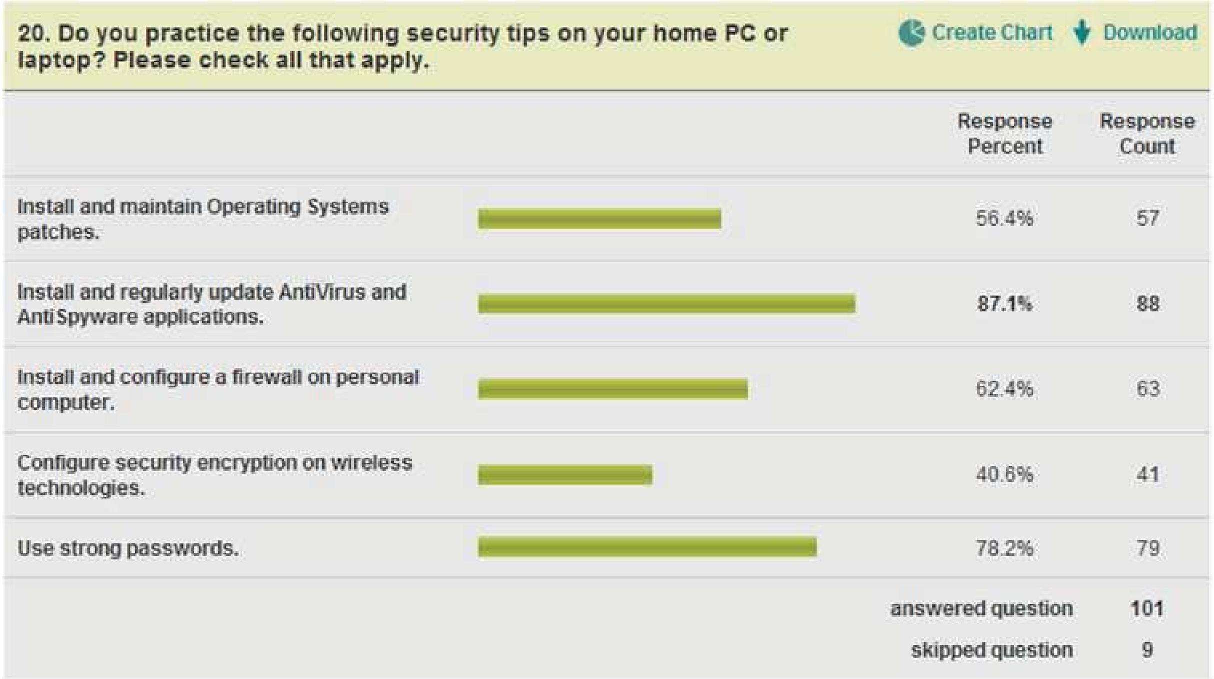
18. Do you happen to have a firewall installed on your home computer?

	Response Percent	Response Count
Yes	75.7%	81
No	24.3%	26
	answered question	107
	skipped question	3



19. Do you know what to do to protect yourself against identity theft?

	Response Percent	Response Count
Yes	59.4%	63
No	40.6%	43
	answered question	106
	skipped question	4



20. Do you practice the following security tips on your home PC or laptop? Please check all that apply.

	Response Percent	Response Count
Install and maintain Operating Systems patches.	56.4%	57
Install and regularly update AntiVirus and Anti Spyware applications.	**87.1%**	88
Install and configure a firewall on personal computer.	62.4%	63
Configure security encryption on wireless technologies.	40.6%	41
Use strong passwords.	78.2%	79
	answered question	**101**
	skipped question	9

Glossary

Antivirus - a utility that searches a hard disk for viruses and removes any that are found.

Browser Hijacker - a specific type of spyware that will allow a hacker or malicious perpetrator to spy on the infected computer's Internet browsing activity.

Identity Theft - the appropriation of an individual's personal information to impersonate that person in a legal sense.

Keylogger - a hardware device or a software program that records the real time activity of a computer user including the keyboard keys they press.

Peer To Peer (P2P) – Computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server.

Personal Digital Assistant (PDA) - a handheld device that combines computing, telephone/fax, Internet and networking features.

Pharming - a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent.

Phishing - an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients.

Spyware - any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes.

Trojan Horse - a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

Virus - a program that secretly attaches itself to another document or program and executes when that document or program is opened.

Wardriving - the act of driving around in a vehicle with a laptop computer, an antenna, and an 802.11 wireless LAN adapter to exploit existing wireless networks.

Wired Equivalent Privacy (WEP) - a security protocol for wireless local area network (WLANs) defined in the 802.11b standard.

Wi-Fi Protected Access (WPA) – A security protocol for wireless 802.11 networks from the Wi-Fi Alliance that was developed to provide a migration from WEP.