Prime Scholars Library

Frontiers of Law, Political Science and Art

Review

Vol. 7 (3), pp. 32 - 44, April, 2019

Available online at
https://primescholarslibrary.org/

An investigation of fraud: Motives, related cheats, strategies and avoidance

Murat Sakir Erogul

Califonia University, USA

Abstract

This paper is a conceptual review of the major crimes leading to ID fraud and losses of millions of dollars for business and people in the world every year. The paper provides a review of the unique effective techniques for sustainable development of prevention methods that have been offered to people and business. In addition, the paper reviews literature and summarizes the most effective ways for people and business to protect them against ID theft because victims may face a lengthy process of cleaning up the damage, such as their reputation, credit rating, and jobs. Identity (ID) theft is unauthorized obtaining of others confidential information in order to misuse it. ID theft is one of the major problems that impose billions of dollars annually on people and businesses across the globe. In 2008 only, 9.9 millions of Americans were victimized which show 22% increase compared to 2007. Analyzing four major factors - political, economic, social, and technological- reveals that social and technological factors are the significant origins of ID theft. Social engineering is a technique for thieves by which social engineers take advantage of people's behaviors in social networks such as Facebook to steal individuals' key information. This report examines different types of frauds that are the major outcomes of ID theft. The frauds as the results of ID theft comprise ID fraud, financial fraud, tax fraud, medical fraud, resume fraud, mortgage fraud, and organized crimes such as money laundering, terrorism, and illegal immigration. Moreover, the various techniques that thieves use to attack individuals and organizations are discussed. The different techniques are divided to two major ones, physical and technological. Physical techniques include several traditional ways such as mail theft and insider theft. It is crucial for organizations' managers to know that despite new technology-based techniques, more than 70% of ID theft occurs by insiders. In addition, it will be shown how thieves apply both technology-based techniques such as phishing and social engineering to steal personal information. Finally several effective prevention techniques will be provided for individuals and organization to protect key data and information against identity theft. Usually, thieves attempt to bypass security systems through human elements. Therefore, the recommendation significantly emphasizes developing individuals' awareness through public and organizational training.

Keywords: Identity, theft, fraud, prevention, personal information.

INTRODUCTION

Organizations and people should be cautious in protecting their identity to prevent fraud as a result of ID theft. How sure are they that they will not be one of a million victims of ID fraudsters in 2010? The Federal Trade Commission reported that 9.9 million (22% more than 2007) Americans suffered from identity theft in 2008, and stated that "ID theft costs consumers about $50 billion annually" (Finklea, 2010: 1).

In spite of the attempts to enforce the law, the number of new identity (ID) theft victims is increasing everyday across the globe. ID theft "can refer to the preliminary steps of collecting, possessing, and trafficking in identity information for the purpose of eventual use in existing crimes such as personation, fraud, or misuse of debit

card or credit card data"(justice.ca, 2010). According to CIPPIC[1], identity thieves tend to steal twelve types of private personal information stated as follows (CIPPIC, 2007: 1):

1. Credit card numbers
2. CW2 numbers (the back of credit cards)
3. Credit reports
4. Social Security (SIN) numbers
5. Driver‟s license numbers
6. ATM numbers
7. Telephone calling cards
8. Mortgage details
9. Date of birth
10. Passwords and PINs
11. Home addresses
12. Phone numbers

Moreover, Appendix 1 provides several examples of personal private information that identity thieves attempt to steal.

Based on its definition, ID theft usually is associated with fraud and causes losses for victims, including individuals and corporations. According to the Canadian Council of Better Business Bureaus, Canadian consumers, creditors, banks, businesses, and stores lose more than $2 billion every year because of ID theft (justice.ca, 2010). In addition, the UK's Fraud Prevention Service (CIFAS) reports that the rate of ID theft in the UK is growing, and it causes a loss of £1.7 billion in the British economy every year (CIFAS, 2010).

As can be seen, ID theft is one of the major crimes leading to ID fraud and losses of millions of dollars in the world every year. It is important to understand effective ways to protect people and corporations against ID theft because victims may face a lengthy process of cleaning up the damage, such as their reputation, credit rating, and jobs. Therefore, analyzing the main possible factors such as political, economic, social, and technological and how they may increase or decrease ID theft is necessary. In addition, since people and corporations need to know how to prevent fraud as a result of ID theft, ID theft techniques, ID fraud, and methods of ID fraud prevention will be examined.

POLITICAL, ECONOMIC, SOCIAL AND TECHNOLOGICAL (PEST) ANALYSIS

In order take effective actions to prevent and decrease ID theft in a society, it is necessary to scan and analyze the external or micro-environmental factors. PEST analysis is one of the main frameworks that help to evaluate how political, economic, social, and technological factors affect ID theft.

[1] CIPPIC: The Canadian Internet Policy and Public Interest Clinic (CIPPIC) is a legal clinic of that was established at the University of Ottawa, Faculty of Law in the fall of 2003.

Political and economic factors and ID theft

Lack of political and economic stability in developing nations significantly increases ID theft, especially in developed countries. Every year millions of people from developing countries in which people suffer from poverty or political issues immigrate to the developed countries (UNHCR, 2007). Statistics show that more than 10 million illegal Mexicans, South and Latin Americans, and Asian immigrants live in the USA (Passel, 2006: 2-3). The American society is burdened by the cost of illegal immigration in form of ID theft because Illegal immigrants steal identities such as social insurance number or drivers licence in order to work (Sullivan, 2006). For example, on March 2007, the U.S. District Court on immigration sentenced 20 unauthorized Mexican immigrants who committed ID theft, document-fraud, and misusing Social Security numbers (ICE, 2008). As it can be seen, unfavourable political and economic situations encourage people to immigrate illegally, which lead to ID theft and ID fraud.

Social factors and ID theft

Social environment and factors, such as habits and communication by social networks have major effects on ID theft. The level of peoples‟ knowledge about the use of social networks and their role in protecting privacy is important in a society, especially in the .com arena. Companies, institutions, and people try to protect their privacy, confidential data, and personal information by applying the various security mechanisms. However, social engineering "is alive and well, and probably remains the most effective hacking technique" to obtain privacy and confidential information. According to Applegate, social engineering is a "methodology that allows an attacker to bypass technical controls by attacking the human element in an organization" (Applegate, 2009: 1, 40).

Since communication through social networks, such as Facebook, Twitter, and Skype is growing, social engineers remain a potent threat to people‟s cultural attitudes and behaviours in social networking. A survey by the point for credit union research (2008) and advice in the U.S.A, Canada, the United Kingdom, France, Germany, and Spain in 2008, illustrates that:

(i) 25% of Germans and 60% of Americans have shared their account passwords with a friend or family member. As result of this cultural attitude, 3% of Germans have experienced ID theft.
(ii) 50% of Americans use family member names, important dates, nicknames, or pet‟s name as online accounts passwords.
(iii) In all six countries, about 40% of consumers display their personal information in their social network profile and some of them use exactly the same information as their passwords.

(iv) More than 25% of consumers in France use their displayed date of birth in social network as their online passwords.

Consequently, attackers can freely obtain this information in users‟ profiles. Attackers apply this information to receive complementary information without raising any suspicion for a final attack, ID theft and fraud. For example, a social engineer obtains a financial manager‟s information in a social network so that the attacker knows that manager‟s first and last name, career, and birth of date. The following conversation can be a way to steal his/her ID over the phone:

Mr. Hyman: Hello?
Caller: Hi, Mr. Hyman, this is Bob in IT tech support. Due to some disk space limitation, we are going to move some user‟s directories to another disk at 5:00 pm today. Your account will be a part of that, and will not be available temporarily.
Mr. Hyman: Uh, thank you very much that would be good because sometimes my computer is slow. No worries, I will not be here by then.
Caller: Awesome. Please make sure to log off before leaving. I just need to check a couple of things. Your user name still is Hyman, right?
Mr. Hyman: Yes. It is Hyman. None of my files will be lost, will they?
Caller: No sir. But I will check your account now ensure everything will be OK. What was the password on that account, so I can check your files?
Mr. Hyman: Sure, My password is Saturday20, with the first letter capitalized.
Caller: Great, Mr. Hyman, I appreciate your help. I will make sure to check you account and verify all the files are there.
Mr. Hyman: Thank you very much. Bye.

In this example, the manager trusted the caller only because of some primary but important information about him in his profile in a social network. In this conversation the social engineer takes advantage of the manager‟s trust because he posed as an insider and his tendency to be helpful. In addition, fear of having more technical problems encouraged him to cooperate and to give all the information. As result, the caller could get all other crucial information over the phone, which may cause numerous huge financial frauds through his ID. As it can be seen, a social engineer could bypass a strong security mechanism through a manager as the weakest part of the security chain. As result, social factors such as the widespread use of social networks that are unsecured sources, habits, and customs make people privacy vulnerable to ID theft.

Technological factors and ID theft

Technological factors threaten people and institutions‟ privacy and increase ID theft as long as they use new technology without using a proper security system, and follow their dangerous behaviours at work or social networks. The advent of new technology, such as PDAs, cell phones, USB, Wireless, and laptops in the World Wide Web arena has changed people‟s behaviour to manage their private information, such as credit cards and social insurance numbers. No matter where people are online and work, they are not 100% safe when they use their private information such as banking account information. Today, fraudsters consider the Internet as a new frontier, easy accessible, and a goldmine of private information to steal people‟s ID (Motsay, 2010). According to Mostay (2010), people and institutions lose around $40 billion annually in online activity through ID theft and communication fraud.

In addition, almost 80% of financial institutions apply wireless technology such as smart phone (Blackberry devices) in their operation while only 75% of devices are using mobile safeguards (CardLine, 2007). Therefore, it is crucial that people change their behaviours when they use new technologies such as wireless or online banking. For example, saving the online banking username and password in the browser is one of the biggest mistakes. In the new technology boom, individuals and technology managers must change their attitudes and behaviours and consider precautionary solutions when using new technology. For example, applying appropriate security systems, such as not saving account information in computers, using anti spy-ware programs, and wireless safeguards will protect people and individuals against ID theft. Consequently, new technology threats and their effects on ID theft differ based on individuals and managers‟ behaviours and the precautions they take.

ID THEFT AND OTHER FRAUDS

According to Gercke (2007), ID theft is often the first and preparation phase to the second phase. Accordingly, the major motives of perpetrators for stealing identities are:

1) Requirement of further fraud (in most of cases)
2) Sell the stolen information
3) Hiding the identity

Moreover, ID fraud, financial fraud, tax fraud, medical fraud, resume fraud, mortgage fraud, and organized crimes such as money laundering, terrorism, and illegal immigration are the significant outcomes of ID fraud. Facts show that every year ID theft and related fraud imposes overwhelming costs on nations. For example, the United Kingdom is annually burdened about £1.3 billion from ID related fraud that includes: tax fraud for £215 million, credit fraud for £215 million, money laundering for £400 million, and immigration fraud (forging passports) for £584 million (Whitley et al., 2007:

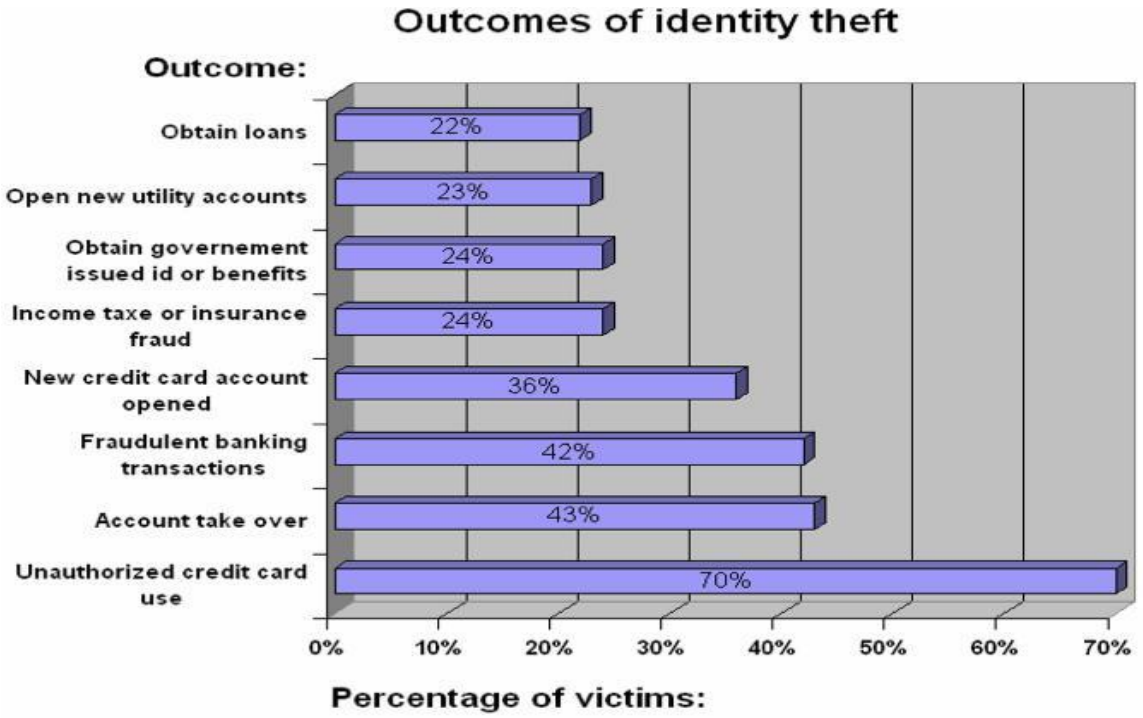

Figure 1. The major outcomes of ID theft Canadian people suffered from in 2006 (CIPPIC, 2007: 23).

53-54). ID theft is usually the primary main step associated with other types of fraud. A brief definition of all types of fraud
and a deeper discussion about a few of them, which are reported by CIPPIC (2007: 23) (Figure 1).

ID fraud (forging identity documents)

Personal information is used to create fake driver‟s licenses, vehicle registration certificates, credit and debit cards, and other identity documents that will be used to commit fraud.

In October 2005 in Toronto, a theft ring created forged health cards, credit cards, driver‟s licenses, and other key identities to open new bank accounts.

Financial frauds

Taking over existing accounts: Fraudsters with enough personal information can contact organizations and take control of the existing bank account and withdraw all money in a shortest period of time without any suspicion.

Opening new accounts: With having private informationand ID such as name, address, and social insurance numbers, fraudsters can open new bank accounts, credit accounts (credit cards, lines of credit, or loans), in-store accounts, cell phone accounts, and student loans accounts under the victims‟ real information; they then will change their billing address in order to conceal their activities from victims. In such cases fraudsters have more time and more opportunities to commit fraud and in most of cases, victims only will realize when collector agencies contact them or their credit applications are refused.

Online shopping: In this method fraudsters shop onlinewith victims‟ personal information and ID in a different area, usually Africa, and ask to deliver orders to a trusted third party. They then request repackaging of orders and shipping them to the fraudsters. This method of fraud increased in Canada in 2003, when an Albertan purchased merchandise online with a stolen ID and credit card number and asked for his order to be shipped to North Dakota and re-shipped them to Edmonton through repackaging.

Mortgage fraud: A new disturbing form of fraud that hasbeen growing recently, which is another result of ID theft. Mortgage fraud is defined as obtaining mortgage financing under a fake ID or false identification. In this way fraudsters use stolen IDs, such as falsified ID, income statements or employment records to take ownership of properties and sell them or take out mortgage under victims‟ names and credits. According to CIPPIC (p.28), mortgage fraud increased 500% in the U.S.A from 4,000 cases in 2001 to 17,000 cases in 2004. In addition, Canadians annually lose $1.5 million due to mortgage fraud. For example, in April 2006, in Surrey

B.C., a woman posed as the owner of a property and applied for a $170,000 mortgage. A mortgage broker arranged a mortgage but another broker informed police after identifying the scam (CIPPIC, 2007: 29). In addition, based on Ottawa Police service, mortgage fraud involves other crimes as well; drug trafficking is one of the major ones. Accordingly, drug traffickers own properties through ID theft and mortgage fraud; they then use these properties to grow marijuana, which caught the attention of neighbors in most of the cases (CIPPIC, 2007: 29).

The Canadian Criminal Intelligence Service (CISC) investigated the negative impacts of the mortgage fraud on Canadian society and its economy and the result of the survey is illustrated as follow (CIPPIC, 2007: 7):

"In terms of social harms, mortgage fraud can cause significant psychological or mental stress to the victims. The consequences to victims can include guilt and shame, disbelief, anger, depression, a sense of betrayal and a loss of trust. Individuals can also spend a considerable period of time recovering lost or stolen identification and repairing damaged credit histories. Multiple mortgage frauds within a neighborhood can result in inflated neighborhood property values, higher property taxes, an inability to sell homes, and abandoned properties.…
In terms of economic harm, the corruption of professionals in the real estate and mortgage industries is difficult, expensive and time consuming to investigate.…

The average mortgage fraud loss per property was approximately $100,000.
One challenge is that the healthy real-estate market has caused housing prices generally to increase. As a result, it is sometimes difficult to detect fraudulently over-valued properties. However, after a real-estate market downturn, the prices of some of these fraudulently over-valued properties will fall. As a result, defaults will occur and some frauds will be readily apparent."

Resume fraud

Since criminal record checks are one of the main prerequisites of secure positions particularly in government sections, fraudsters use stolen identities to get employment (CIPPIC, 2007). Resume fraud is an opportunity for fraudsters to use individuals‟ appropriate related experiences and education. The worst situation in resume fraud is that fraudsters secure a position in a strategic government section such as the Canada Revenue Agency. In this situation the aftermath will be irreparable because thieves have access to the most important private information. For example, Michael Ritter, the Albertan fraudster claimed that he graduated from London School of Economics (LSE) and secured his positions for almost five years as the chief parliamentary counsel at the Alberta legislature. Although Ritter did not use a stolen ID to forge his resume, it is possible for ID thieves to do the same as what Ritter did to secure an important position and gain benefits.

Immigration fraud (obtaining a passport) and terrorism

International criminals, such as terrorists and illegal immigrants, use stolen identities to obtain a passport to cover their felonies and illegal activities. These types of fraud often count as a significant threat for national securities across the globe. For example, in July 2002, a member of al-Qa'ida, who was using Australian passport, was arrested in Canada. He was charged by the government of the Netherlands because he planned to blow up the American embassy in Paris (OCBA, 2010). In addition, according to the FBI, Al-Qaeda‟s members purchased their cell phones and paid by stolen identity and credit cards in Spain. They also stole ID and forged passports to open bank accounts in which terrorist supporters were transferring money from Afghanistan and Pakistan (Arterberry, 2005).

Medical fraud

Medical fraud happens when someone steals important information or ID such as health cards, and uses them to claim or obtain medical services under the victim‟s name. One of the possible results of medical fraud is misleading health services providers, which may put a patient‟s life at risk. Statistics shows that around 500,000 Americans have been victims of medical fraud. Although this statistic is not available for Canada, the Ontario Ministry of Health and Long-Term Care claims that medical fraud (health care fraud) is the main outcome of the ID theft in Ontario (CIPPIC, 2007: 26).

Tax fraud

ID fraudsters use victims‟ identities such as employment records or social insurance numbers to file their income taxes to receive victim‟s tax refunds (CIPPIC, 2007). For example, according to the United States District Court (2010), District of Arizona, a group of fraudsters filed income tax returns by stolen IDs between 2005 and 2008 and obtained about $4 million in tax refunds.

THEFT TECHNIQUES

According to CIPPIC, ID thieves may steal personal and private information in various ways, ranging from simple (physical) ways such as theft of wallets to very sophisticated methods (technology-based thefts) such as

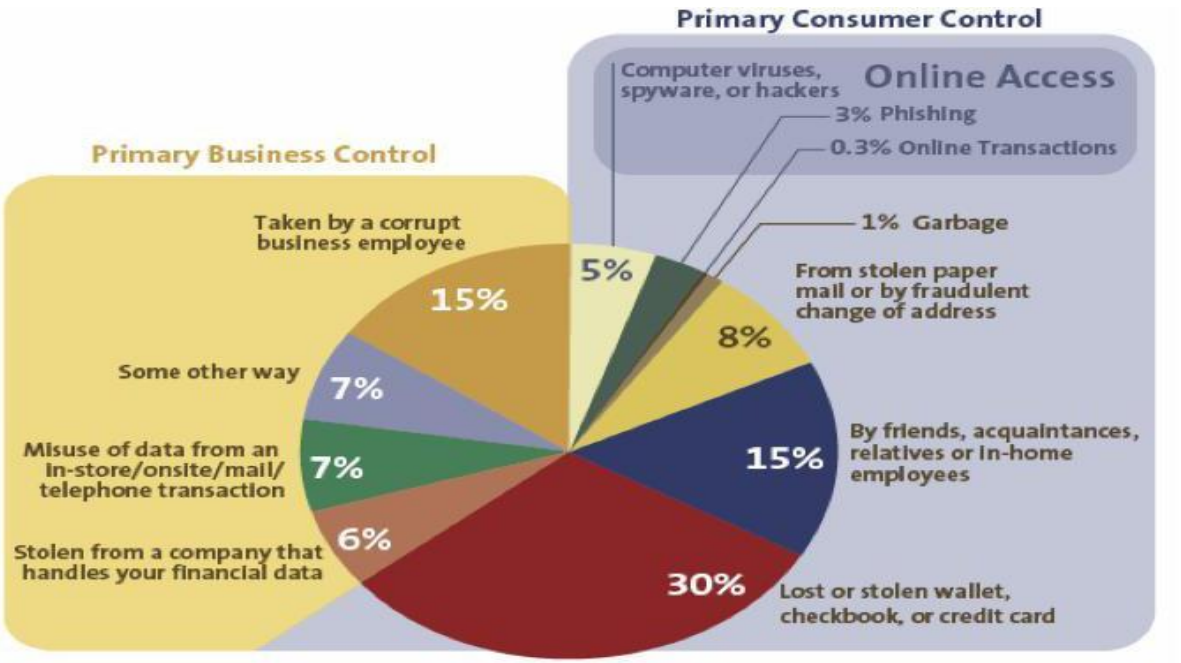

Figure 2. The different techniques, frequency, and distribution of ID theft in the United States in 2006 (CIPPIC,2007, p.4).

computer hacking. In addition, the CIPPIC (2007) report illustrates that ID thieves may steal people‟s private information through third parties. Statistics show that ID theft through high-tech methods such as the internet is less than 10%; however, identity thieves significantly use low-tech methods to steal personal information. Figure 2 illustrates the different techniques, frequency, and distribution of ID theft in the United States in 2006 (CIPPIC, 2007: 4).

In order to deal with ID theft it is crucial for individuals and organizations to understand various techniques; therefore, different techniques from physical to high-tech, which were retrieved from the CIPPIC report in 2007.

Physical theft techniques

Theft of personal information sources (wallets, cell phones, and computers)

Today, thieves can obtain personal information by stealing rich sources of information particularly laptops from important governmental information centers such as Canada Revenue Agency, CRA. The following examples are some of the most important ones (CIPPIC, 2007: 5):

“-On Friday, September 26, 2003, two well dressed men walked into the Calgary offices of the Canada Customs and Revenue Agency (CCRA) and stole 15 DELL laptop computers valued in excess of $60,000.00.
(i) Four computers containing confidential personal information of more than 120,000 Canadians were also stolen from CCRA‟s Laval offices on September 4, 2003.

(ii) In May 2005, the U.S. Department of Justice reported that a laptop containing information on 80,000 departmental employees was stolen.
(iii) A similar situation occurred at the University of California, Berkeley. This time, personal information, including social security numbers (SSN), was stored, unencrypted, on the laptop.”

Trash-theft

The ID thieves can receive personal information through diving in household trash as well as that of specific businesses such as hotels, rental car companies, and restaurant. In this way ID thieves may obtain personal information on discarded financial receipts.

Change of address

Since mail is a good continuous source of personal information and it takes more time until victims detect any theft, ID thieves can redirect mail to obtain victims account information. For example, in March 2006, two fraudsters who used a change of address form to redirect people mail were arrested in Ottawa. According to police, victims provided all personal information and replied. Finally, police were alerted about the fraud by Canada

Post Corporate Security.

Mail theft

Mail theft is an easy way by which thieves can steal key information from businesses or home mailboxes, recycle bins, or garbage. Thieves may obtain personal information through bank and credit card statements, utility bills, or driver‟s licenses. According to a survey, a majority of law enforcement officials (68%) believe that mail theft is the significant concern of ID theft in the U.S.A. For example, in 2004, Bradley, a thief who committed mail theft was sentenced to four and half years because he used stolen information to forge other documents for further fraud (CIPPIC, 2007: 7).

Tombstone theft

By this technique ID thieves collect all personal information such as birth date and full names of deceased from newspapers and tombstones. In the next step, thieves pose as deceased‟s insurance company and collect other important personal information from funeral homes. For example, in Atlanta in 2007, thieves purchased the identities of 80 deceased for $600 each and secured $1.5 million in car loans (CIPPIC, 2007: 9).

Skimming (magnetic strip duplication)

Using this method, thieves use a small electronic device called a “skimmers” that can copy credit or debit card information after swiping the card. Since any cards with a magnetic strip such as library cards are programmable, thieves then can create additional cards by using stolen information for fraud. For instance, in Calgary in 2004, thieves copied 35 ATM users‟ debit cards in an hour (CIPPIC, 2007: 9).

Insider theft

Dishonest insiders in organizations that hold people‟s key information, such as credit and debit card numbers often may steal personal information due to lack of appropriate internal control. Findings in a study show that up to 70% of the ID theft from American organizations is committed by insiders (CIPPIC, 2007: 11).

Purchasing stolen personal information

One of the easiest ways to receive an individual‟s private information is to purchase information from insider thieves, or data traffickers. For example, thieves sold the 35 duplicated debit cards (in Skimming) and earned $117,000 (CIPPIC, 2007: 13).

Technology-based ID theft techniques

Phishing

“Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party” (Jagatic et al., 2005: 1). Jagatic et al. (2005) state that social networks, such as Facebook, Orkut, LinkedIn, MySpace, and Friendster are the main sources for mining information about victims (Jagatic et al., 2005: 2). According to CIPPIC, since phishing messages are attractive for people, thieves use them in up to 25% of ID theft. Thieves in phishing messages usually ask for private information to fix, update, or resolve other technical issues (Appendix 2). Experts state that in phishing messages, surprisingly, thieves use fraud alerts to trick individuals. When phishing messages come with the same logos and colors of the trustworthy organization it is called Spoofing. Statistics show that 24% of Canadians received phishing messages that ask for their account information, and 14% of them became victims (2007: 13-14). In addition, 57 million Americans received phishing message in 2003 and more than 50% who responded were victimized by ID theft (Litan, 2004: 1). For example, in Romania, police arrested Dan Marius Stefan who stole $500,000 through phishing (Mitchison et al., 2004: 33).

Hacking

Unauthorized access to systems or databases to obtain personal or organizational classified information is called hacking (Paget, 2007). Hackers can sell all stolen information or gain profit from private information directly. For example, in 2009, a computer hacker, Gonzalez, 28, stole more than 135 million credit and debit card numbers in chain stores like 7-Eleven, and obtained $1.6 million in cash (Meek, 2009).

Wardriving

In wardriving, thieves attempt to search, detect and connect to individuals or organizations‟ unsecured Wi-Fi or wireless networks and steal personal information. Thieves or “war drivers” use devices with wireless networks detectors such as notebooks or PDAs to connect to unsecured networks when they drive in neighborhoods (CIPPIC, 2007). For example, in 2003, Salecedo the American hacker and his partner were sentenced to nine years in prison because of unauthorized

access to Lowe‟s Companies‟ wireless connection and stealing credit card account numbers (Justice, 2004).

Social engineering techniques

As was mentioned earlier, ID thieves attack the human elements especially in organizations to bypass technical controls and steal personal information. “Social engineering involves exploiting the natural tendency of a person to trust others, especially people with whom they have some sort of relationship” (CIPPIC, 2007: 20). Following are several main typical techniques that are used by social engineers:

Pre-texting

In this form of ID theft, social engineers rely on “smooth talking” to target victims or third parties to steal personal and private information (CIPPIC, 2007). According to CIPPIC (2007), typically pre-testers use several methods to steal personal information as followed:

1) Contact third parties and pose as an internal employee or another company on behalf of victims and ask for their accounts information.
2) Pretend to do a telemarketing survey in which the victim‟s information is a part of survey requirements.
3) Pretend to from call an anti fraud organization and victims‟ information is required to register in protection programs.
4) Trick youth and children and target them to obtain personal information in internet chat rooms.

For example, in Canada in 2004, ID thieves called Equifax Canada Inc.[2], posed as a legitimate credit grantor, and managed to steal 1400 Canadians‟ credit files (CIPPIC, 2007: 21).

Obtaining credit reports

Since credit checks for some situations are usual, thieves use this way to steal personal information. In this form of ID theft, fraudsters pretend to be a landlord, car dealer, or potential employer and obtain individuals private information.

Fake employment schemes

In this form, bogus employers post jobs on their websites and ask job seekers to submit a resume or an application form to obtain personal information. With this technique, in Ottawa in 2006, thieves obtained personal information such as SIN and driver‟s license numbers (CIPPIC, 2007: 21-22). In B.C. in 2003, with using the same techniques, a fraudster stole personal information, opened a bank account, forged cheques, and obtained $80,000 (CIPPIC, 2007: 22).

THEFT PREVENTION

Fraudsters use different methods and strategies to obtain personal information. In fact, based on the situation, thieves choose their methods to attack to their targets. For example, the ID techniques for stealing information from organizations differ from individuals. Therefore, appropriate prevention techniques that are recommended by Royal Canadian Mounted Police (RCMP) (2010) for individuals and organizations are as follows:

Prevention techniques for individuals

1) Since thieves are able to steal personal information via the Internet, fax, regular mail, or telephone, individuals should not disclose personal information when they are not hundred percent sure.
2) It is recommended to carry entire identities document only when is needed; otherwise should be kept in a safe place.
3) Ask for periodical credit check reports from banks, creditors, or other financial institutions and report any irregularities to the credit bureaus.
4) It is recommended that individuals do not allow others such as cashiers to swipe their credit and debit cards.
5) Personal identification number when using a PIN pad or an ATM should be covered.
6) It is better to memorize all personal ID numbers such as debit cards, and telephone calling cards and never write them on the cards.
7) It is better that individuals be familiarized with their credit and debit cards billing cycle and monitor them carefully.
8) Document shredding before discarding in trash bins is strongly recommended because garbage and trash bins are a goldmine for thieves.
9) The post office and other relevant financial institutions should be informed about any address change.

Among all of these, all mail should be removed quickly from mailbox and a vacation hold when people travel is recommended (Paget, 2007). It also is recommended to review financial account balances and check into any unexplained withdraw or charges (Paget, 2007).

In addition, according to Paget, the following techniques are recommended to individuals to protect personal information in computer or online networks:
a) Individuals should watch out for phishing messages and not disclose personal information.
b) Reputed and accredited business never request

[2] Equifax Canada Inc is one of the Canadian major customer reporting agencies.

account information such as user name, passwords, social insurance numbers, and credit or debit cards numbers; therefore, these e-mail or contacts should be rejected.
c) It is recommended that people neither use links in unknown emails, nor cut and paste them in their web browsers because phishers can access their computers after open those links.
d) Using comprehensive security software such as anti-virus, anti-spyware, and firewalls and keeping them up to date is recommended.
e) People should ensure that their security software is enabled and check all attachments in their email when they decide to download attached files regardless of who is the sender.
f) People should not share their personal email with their family or friends and post their address and personal information in their website or social networks.
g) It is not recommend that individuals send personal information even to friends and family because their computers might not be protected.
h) All personal information should be deleted permanently in old computers or hard drives be formatted before disposing of a computer.
i) All web sites and their components such as URL and locked icon, and their privacy policy should be check whether are secured and correct or not before providing personal information.
j) Using strong passwords is strongly recommended to people in online networks. Security experts believe that strong passwords are made by more than six characters and are a combination of letters, numbers, and special characters such as Hd4vK%j.

Prevention techniques for organizations

Since businesses and organizations carry people‟s identities and private information in their databases, it is necessary to have a strategic plan to protect key information. At first phase, to have an effective and secured system, organizations, such as financial or governmental organizations, must assure that red flags can be detected by their security mechanisms.
In March 2009, the Federal Trade Commission (2010) provided a guideline, the red flags rule. Accordingly, identity theft prevention programs should be provided and cover the following major elements:

1) First: Reasonable policies and procedures to identify the “red flags”.
2) Second: Detect the identified red flags.
3) Third: appropriate actions after detection of red flags.
4) Fourth: Evaluate and update the prevention program periodically.

Moreover, according to Collins, despite common thought, the majority of ID theft happens in workplace rather than online. Collins states that employees or individuals who pose as employees commit more than 70% of ID thefts in organizations; therefore Collins recommends the following prevention techniques to organizations (Collins, 2003: 304-305):

a) To secure organizations with an appropriate and effective personnel selection policy to hire honest persons.
b) To apply a risk assessment process.
c) To conduct an e-business risk assessment tool to identify red flags to ID theft.
d) To require that all documents that contain identities and sensitive information about individuals and business be shredded before disposing.
e) To develop and train employees to recognize fake applications.
f) To enhance ethical culture of organization.
g) To reward and support employees who endorse honesty in organization.

In addition, the following prevention techniques are recommended to organizations by François Paget (2007), Senior Virus Research Engineer in McAfee to avoid ID theft:

a) To appoint a person to be responsible for organization security system.
b) To decrease risky behaviour such as sending and receiving email without discretion and downloading programs through training, listing users responsibilities, and documenting the rules of the information system and networks.
c) To build a secured network and install secured hardware and software.
d) To adopt manageable solutions for employees who are responsible to support the system.
e) To manage the organization network by documenting all activities, such as troubleshooting, installing, testing, and restoring.
f) To formalize the usage of the corporate network, such as adding or deleting users.
g) To use prevention security systems to identify, detect, block, and report suspicious online activities.
h) To install reliable security systems, such as anti-virus, anti-Trojan, and anti-spyware) on all terminals (servers and workstations) that connect to corporate network.
i) To update all security software regularly.
j) To assess, modernize, reconfigure, and administer corporate security system.
k) To ignore any free remote security system audits
l) To protect all data backup devices in organization
m) To avoid carrying crucial data and information onto portables computes such as laptops.
n) To analyze, monitor, and control the corporation wireless network and devices.
o) To protect organization information system by limiting

physical access to the computers.
p) To minimize the risks of copying or stealing of key data by supervising employees turnover and job mobility.
q) To control information flow outside of the corporation electronic network such as interviews, responses to any questionnaires, presentations in conferences, and information exchanges in private or public.

CONCLUSIONS AND RECOMMENDATIONS

Identity theft as a major crime is increasing across the globe, threatening people and organizations. Thieves, fraudsters and criminals use various techniques to obtain people‟s private information. The variety of techniques to acquire personal information, and amount of profit reflect the level of motivation, expertise and commitment of fraudsters. Facts show that criminals alter their techniques based on their motive; therefore, the costs of ID theft to individuals are different than to organizations. As mentioned before, social and technological factors are major motives for perpetrators. These two factors are tied together and increase the identity theft. In addition, emerging new technology and the lack of enough people‟s knowledge about how to protect their personal information motivates fraudsters. Accordingly, it is anticipated that identity thieves move towards using new techniques to obtain personal information particularly in online environment. Therefore, it is crucial to enhance people‟s knowledge about how to protect themselves in online networks through education in the media. In terms of costs of public education, it is necessary to mention that the governments and other big corporations should consider costs as an investment rather than expenditures to make a safe society.

Moreover, organizations that collect people‟s personal information in their databases such as banks, financial institutions, and retail stores are more vulnerable than other small businesses or corporations. Therefore, it is vital for these institutions to have appropriate strategies, policies, and actions to protect them against mass identity theft. The good defensive strategies should combine security awareness, training, technical control, and an effective information management strategy. Facts show that identity theft by insiders is a major problem for organizations; thus organizations should consider a strong and effective internal control to avoid identity theft. It is recommended that organizations educate employees about the most pervasive attacks, social engineering, and its consequences. Additionally, managers should notice that poor performance and neglecting of the damage of potential attacks not only imposes huge amounts of loss but also destroys the image of corporation.

Individuals and organizations must accept that they are vulnerable to identity theft; therefore, applying the most effective security system should be associated with developing awareness about possible threats because “awareness is the best defense”.

REFERENCES

Applegate S (2009). Social Engineering: Hacking the Wetware!. Information Security Journal: A Global Perspective, January, 18(1): 40-46. Available from: Business Source Complete.

Arterberry JD (2005). Identity Theft: Trends, Techniques, and Responses [Internet], Washington, The United States Department of Justice: Criminal Division. Available from: <www.nacrc.org/events/.../idtheftnacojuly05.pdf> [Accessed 26 May 2010].

CIFAS (2010) Identity Theft – Victims [Internet]. London, The UK‟s Fraud Prevention Service (CIFAS). Available from: <http://www.cifas.org.uk/default. asp?edit_id=577-57> [Accessed 25 May 2010].

CIPPIC (2007). Working Paper No. 2: TECHNIQUES OF IDENTITY THEFT [Internet], Ottawa, Canadian Internet Policy and Public Interest Clinic (CIPPIC).
Availablefrom:
<http://www.cippic.ca/documents/bulletins/Techniques.pdf> [Accessed 25 May 2010].

CISC (2007). Mortgage Fraud & Organized Crime in Canada [Internet], Ottawa, Criminal Intelligence Service Canada (CISC). Available from: <www.cisc.gc.
ca/products_services/mortgage_fraud/.../mortgage_e.pdf>[Accessed 25 May 2010].

Collins JM (2003). Business Identity Theft: The Latest Twist. Journal of Forensic Accounting, 4: 303-306.

Finklea M (2010). Identity Theft: Trends and Issues Kristin [Internet], Washington, The Federation of American Scientists (FAS). Available from: <www.fas.org/sgp/crs/misc/ R40599.pdf> [Accessed 25 May 2010].

Federal Trade Commission (FTC) (2010). Fighting Fraud With The Red Flags [Internet]. Washington, The Federal Trade Commission (FTC). Available from: <http://www.ftc.gov/bcp/edu/pubs/
business/idtheft/bus23.shtm> [Accessed 24 May 2010].

Gercke M (2007). Internet-related identity theft [Internet], Strasbourg, Economic Crime Division Directorate General of Human Rights and Legal Affairs Council of Europe Strasbourg Available from: <www.itu.int/.../Internet_related_ identity_theft_
%20Marco_Gercke.pdf> [Accessed 27 May 2010].

ICE (2008). Illegal aliens sentenced on immigration, fraud and identity-theft charges [Internet]. Washington, The U.S. Immigration and Customs Enforcement (ICE). Available from:<http://www.ice.gov/pi/news/newsreleases/articles/080317davenport. htm>[Accessed 26 May 2010].

JagaticTN, Johnson NA, Jakobsson M, Menczer F 2005). Social Phishing. Communications of the ACM, 50 (10) December, pp. 94-100. Available from: Business Source Complete.

Justice CA (2010). „HACKER" INDICTED IN MASSIVE TAX, MAIL, AND WIRE FRAUD SCHEME [Internet], Washington, The Unites States Department of Justice. Available from: <www.justice.gov/usao/az/press_releases/2010/2010-060(Rigmaiden%20et%20al).pdf> [Accessed 24 May 2010].

Justice CA (2004). Hacker Sentenced to Prison for Breaking into Lowe's Companies' Computers with Intent to Steal Credit Card Information [Internet], Charlotte, The Department Of Justice Western District of North Carolina. Available from: <http://www.justice.gov/criminal/cybercrime/salcedoSent.htm> [Accessed 24 May 2010].

Litan A (2004). Phishing Attack Victims Likely Targets for Identity Theft [Internet], Stamford, Gartner, Inc. Available from: <http://www4.gartner.com/resources/
120800/120804/phishing_attack.pdf> [Accessed 23 May 2010].

Meek JG (2009). Hacker Albert Gonzalez charged with largest ID theft ever involving 130M credit, debit cards [Internet], Washington, Daily News Washington Bureau. Available from: <http://www.nydailynews.com/news/national/2009/08/17/2009-08-17_hacker_alberto_gonzales_charged_with_larged_id_theft_ever_in

volving_130m_credit_.html> [Accessed 27 May 2010].
Mitchison N, Wilikens M, Breitenbach L, Urry R, Portesi S (2004). Identity Theft A Discussion Paper [Internet], Brussels, European Commission, Directorate General, Joint Research Center. Available from:<https://www.primeproject.eu/communityfurtherreading/studies/IDTheftFIN.pdf> [Accessed 25 May 2010].
OCBA (2010). Case studies [Internet], Adelide, The South Australian Government's Justice. Available from: <http://www.ocba.sa.gov.au/consumeradvice/ idtheft/studies. html> [Accessed 25 May 2010].
Paget F (2007). Identity Theft [Internet], Santa Clara, McAfee. Available from: <www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf> [Accessed 25 May 2010].
Passel JS (2006). The Size and Characteristics of the Unauthorized Migrant Population in the U.S. [Internet], Washington, Microsoft the Pew Hispanic Centre. Available from: <http://pewhispanic.org/files/execsum/61.pdf> [Accessed 25 May 2010].
Credit Union National Association (CUNA)(2008). Point for Credit Union Research & Advice. 12. November, p.1. Available from: Business Source Complete.

RCMP(2010). Identity Theft and Identity Fraud [Internet]. Ottawa, RCMP. Available from: <http://www.grc-rcmp.gc.ca/scams-fraudes/id-theft-vol-eng.htm>[Accessed 24 May 2010].

Sullivan B (2006). Hidden cost of illegal immigration: ID theft [Internet], New York, Microsoft (MSNBC). Available from: <http://redtape.msnbc.com/2006/03/hidden _cost_of_.html> [Accessed 25 May 2010].
UNHCR (2007). Why do people move to another country? [Internet]. Geneva, The United Nations High Commissioner for Refugees UNHCR. Available from: <http://www.unhcr.org/cgibin/texis/vtx/search?page=search&docid=45efe7852&query=Why%20do%20people%20move%20to%20another%20country?>[Accessed 26 May 2010].
Whitley EA, Hosein IR, Angell IO, Davies S (2007). Reflections on the Academic Policy Analysis Process and the UK Identity Cards Scheme. Information Society, Jan., 23(1): 51-58, Available from: Business Source Complete.

Appendix 1. Types of Personal Information Collected by Thieves.

Personal information:		
Name	**Gender**	**Age**
Date of birth	Place of Birth	Birth certificate
Mothers' maiden name	Marital status	Ethnic origin
Address (current and former)	Telephone number	Email address
Social insurance number (SIN)	Driver's licence number	Health card number
Passport number	Permanent Resident (PR) card	Account credentials (username, password, PIN, etc)
Employment history	Family information	Educational history
Medical history	Number of dependents	Information on your spouse
Property information		
Property Addresses	Vehicle Plate number	
Vehicle registration number	Information on assets	
Financial information		
Credit card numbers	Calling card numbers and personal identification numbers (PIN)	Liabilities
Debit card numbers and personal identification numbers (PIN)	Tax payer identification number	Actual or estimated income
Bank account number	Mortgage details	Investment information
Outstanding debt		
Biometric Information		
Fingerprint	Voice print	Retina image
Height	Weight	Eye and hair color

Source: (CIPPIC, 2007: 2-3).

Visa phishing e-mail[127]

Appendix 2. Types of visa phishing E-mail. Source: (CIPPIC, 2007: 2-3).