2011 Ninth Annual International Conference on Privacy, Security and Trust

The ultimate invasion of privacy: Identity theft

Esma Aïmeur, David Schőnfeld
Département d'informatique et de recherche opérationnelle (DIRO)
Université de Montréal, Canada
aimeur@iro.umontreal.ca, david.schonfeld@insa-rouen.fr

***Abstract*—Identity theft has become one of the fastest growing crimes. Most people are unaware of the amount of data they disclose over all the Internet services proposed by search engines, social networking sites, e-commerce web sites, free online tools, etc. They are also unaware that this data can be easily aggregated, data-mined and linked together, which may lead to a potential identity theft should it fall into the wrong hands.**

If one adds up all of his online searching, communicating, shopping, browsing, blogging, chatting, reading and news sharing, one would realize that one revealed a complete picture of oneself and perhaps some information about his relatives, friends, colleagues, employer, etc. The potential value of this data is considerable for criminals. This paper deals with identity theft and all the issues raised by this type of computer crime. More precisely, it illustrates the variety of information that hackers may want to sift through, the attacks that they may perform and the locations where they can find the information.

***Index Terms*—Identity theft, online vulnerable users, privacy awareness.**

I. Introduction

With the rapid development and advancements in Information Technology, especially the Internet, communications and exchanges between different entities (such as individuals, businesses, governments and information systems) have grown at an increasing speed. However, at the same time the rise of the Information Society has generated a progressive invasion of privacy, which sometimes remains unnoticed. Generally, a malicious person (to whom we refer hereafter as a *hacker*) attempts to commit privacy breach and gathers personal information concerning individuals in order to commit fraudulent acts. When people surf the Web, make purchases or do their banking online, communicate via email or instant messaging, or even visit gaming sites on the Internet, they are regularly exposed to major risks including the violation of their privacy [2,3,4].

As for the hackers, their objectives are numerous; they misuse information for fun, curiosity, for the glory, to inflict damage, for ransom, for revenge, to threaten organizations or for greed. Moreover, they have the feeling of the "behind the PC" impunity and the syndrome of "not seen, not caught". What can a hacker do with your information? Figure 1 presents how victims' information is misused. The hacker can apply for a credit card using your name, use your name to open a mobile phone account or other amenities, apply for a loan or open a new bank account and get cheques. He can also get an official document bearing your name but with his picture, use your name and Social Insurance Number (or Social Security Number in the United Sates—SSN) to obtain government benefits, fill a fraudulent tax return with your information, get a job or rent an apartment. He can even give (or sell) your information to a "colleague" if he is stopped by the police.

In 2010, a twenty-year-old college student hacked Sarah Palin's *Yahoo!* email account by resetting her password. He used only publicly available information from *Google* and *Wikipedia* such as her birth date, zip code and the name of her former high school [A]. The same year, hackers stole the identity of Ronald Noble, Secretary General of Interpol, using fake *Facebook* accounts. They used these accounts in order to get data about ongoing operations [B].

Moreover, the website *FrancoisCharron.com* has uncovered an impressive list of Québec stars fake profiles on *Facebook*. Over a year of research, it was possible to close these fake profiles and thus remove them from *Facebook* [C].

Statistics about identity theft are essentially incomplete. Actually, they come from different sources and the methods of calculation are also different. For instance, institutions and police base their statistics on the number of complaints. However, researchers carry out surveys on the entire population.

According to Ponemon Institute, it is estimated that nearly 1.5 million Americans have been victims of medical identity theft in 2010. In the same vein, the Federal Trade Commission survey reported that 4.6% of the US population were identity fraud victims last year (2010), that is to say about 10 million people [12].

Finally, in only 15 days in March 2011, *Data loss database* reported numerous losses [U]. For example, at the University of York, 17,094 students' names, addresses, dates of birth, emergency contacts, grades, and photos were exposed on the Internet without any login required. At Ortho Montana, a laptop containing 37,000 personal and protected health information records has been lost. At Missouri State University, *Google* indexed 6,030 student names and SSN. Identity theft is therefore a growing phenomenon.

In this non-technical paper, we highlight the concept of identity theft. We begin in section 2 by classifying the types of identity theft. In section 3, we describe the variety of information through which hackers may want to sift. Section 4 and 5 deal with victims, hackers and its impacts. In section 6, we present some techniques that hackers use to steal identities. Finally, in section 7, we examine the legal issues and we present some prevention and protection means for the vulnerable users in section 8.

II. Types of identity theft

According to the definition given by the OCDE, "identity theft occurs when a party acquires, transfers, possesses, or

978-1-4577-0584-7/11/$26.00©2011 IEEE

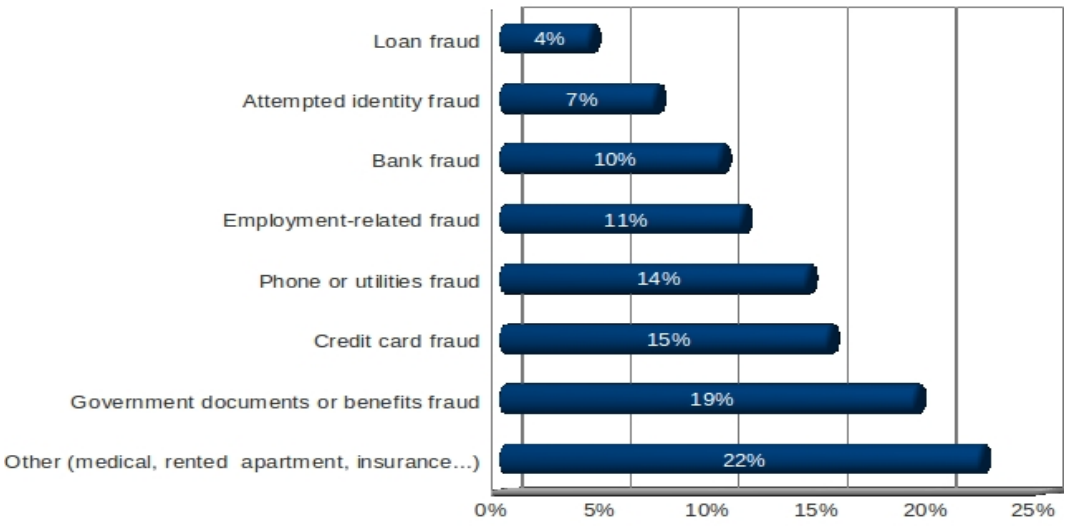

Fig. 1. How victims' information is misused (data from [12])

uses personal information of a natural or legal person in an unauthorized manner, with the intent to commit, or in connection with, fraud or other crimes"[D].

People must understand that identity theft not only affects people using their credit card or debit card, it also includes people who use their name, their Social Insurance/Security Number, online passwords and even their address.

There are eight different types of identity theft. To quote [F] partially, they are as follows: **Financial identity theft** – people are thinking of keeping their money under their mattresses again because their faith in banks and financial institutions are shaken after repeated cases of financial identity thefts. **Medical identity theft** – getting treatment by using somebody else's insurance information is known as medical identity theft. **Criminal identity theft** – here, one person's identity is used to commit a crime. You can find out about this theft if you are caught speeding and the law enforcement officer runs your name and license number through the database. **Driver's license identity theft** – have you ever lost your wallet? If so, then chances are that you might become a victim of this type of theft. Hackers will take your driver's license and sell it to someone resembling you. **Social Security identity theft** – this is one piece of information that can be utilized by many to avoid taxes and other nefarious activities. **Synthetic identity theft** – this is one of the latest types of identity theft in which the thief combines the details of several victims and uses it to create a new identity altogether. **Child identity theft** – kids can also become victims of identity thief, and invariably the perpetrator is a relative, who is sure that the parents will not report him or her to the authorities. **Business identity theft** – in this kind of identity theft, the perpetrator uses the name of a business entity to get loans or a credit extension.

Medical identity theft is most disturbing because it is booming. According to the Ponemon Institute, 1.5 million Americans were victims of medical identity theft and the average cost of treatment is estimated at $20,663 in 2011.

III. Information sought

Three main stages of identity theft [17] are distinguished in the literature. *Initially*, the acquisition of personal information belonging to persons, living or dead, which might come from an ordinary handbag or wallet theft, or a database (even password protected) that can easily be opened by individuals with the expertise and special equipment. *In a second step*, the stolen information will be either sold on illegal markets online where the law of supply and demand will help determine its real value (for hackers), or modified to create synthetic identities. *The third and final step* includes the fraud itself, considering that the possession of personal information belonging to third parties is not considered, by many jurisdictions, as breach of the law [10].

The personal information the hacker wishes to obtain can be as diverse as: *Identifying information* (name, age, gender, address, phone number, mother's maiden name, social insurance/security number, personal identification number (PIN), income, occupation, marital status, place of residence, etc.); *Buying patterns* (stores visited on a regular basis, accounts, assets, liabilities, etc.); *Navigation habits* (websites visited, frequency of visits, pseudonyms used on forums, acquaintances on the net, etc.); *Lifestyle* (hobbies, social networks, travelling behaviour, vacation periods, etc.); *Sensitive data* such as employment, medical or criminal records; or *Biological information* (blood group, genetic code, fingerprints).

From where do malicious people seek their information?

According to Schneier [15], "we leave data everywhere we go. It's not just our bank accounts and stock portfolios, or our itemized bills, listing every credit card purchase and telephone call we make… It's also our lives. Our personal e-mails and SMS messages. Our business plans, strategies and offhand conversations. Our political leanings and positions…"

One should notice that data about individuals gets collected at various places, in various ways and by various means [1]: *By governments*: court records, medical histories, mental health

data, tax returns, financial information, etc.; *By companies you deal with*: for instance your cell phone company knows your location to within a few feet, *Gmail* scans your emails for setting targeted banner ads while *Google Desktop* indexes data from your home and office computers; *By companies you don't deal with*: for example a company called *Acxiom* has recently purchased direct-marketing agencies, background-screening firms, email marketing companies, international data companies, an overseas data-management company and several small businesses from *TransUnion* to continue its expansion into international markets. For another example, consider bankrupt companies, which are often a valuable source for hackers. Moreover, malicious people try to hack social networks [6] and large databases that belong to search engines (*Google*, *Yahoo!*, *AOL*, etc.), data aggregation companies such as the late *ChoicePoint*, online companies such as *eBay* or *Amazon*, and online search tools such as *123people*.

Conti [8] gives a long list of information that *Google* gathers about its users, which is freely disclosed by them when they use the following services: *Alerts* (topics and news stories in which one is interested), *Calendar* (day to day personal and professional schedule), *Catalogs* (items one wishes to purchase), *Earth* (locations of interest), *Gmail* (communications and responses to contacts), *Groups* (groups to which one is affiliated), *Maps for mobile* (one's location), *News* (new stories of interest), *Orkut* (family, friends, and colleagues), *Talk* (contents of communication), *Translate* (native language), *Youtube* (topics of interest), etc. These are only a few examples and the exhaustive list would be much longer [8]. Other search tools such as *123people.com, Whozat.com, Pipl.com, Peekyou.com, PeopleSearch.net* and *Peoplefinder.com* are also good sources of information for hackers in their quest for identity theft. They are free real-time people search tools that look into nearly every corner of the web to provide and gather information.

There are also social network aggregator web sites such as *Lifehacker.com, Spokeo.com, Spoke.com* and *Intelius.com*, which collect data from many online and offline sources (phone directories, social networks, etc.) and have large databases from which they may unwillingly sell to malicious people.

Along the same line, according to [CC], *ChoicePoint.com* (which no longer exists) "combined personal data sourced from multiple public and private databases for sale to the government and the private sector. The firm maintained more than 17 billion records of individuals and businesses, which it sold to an estimated 100,000 clients, including 7,000 federal, state and local law enforcement agencies. However, this data had not been secured sufficiently to prevent theft of data on at least one occasion."

Furthermore, hackers are using websites as a means to attack their users' databases. A typical blog, for instance, contains a large amount of data entered by its user, which is then being shown from the website, such as comments to the latest blog's posts, or discussions. It is crucial for a site owner to distinguish between genuine comments and client-side scripts hidden in a comment entered on his site. Once such an improper payload is displayed on a website, the website becomes the starting point for a variety of attacks. Indeed, just being a member of the network poses risks. When one surfs other sites linked to *Facebook*, for instance, one leaves traces in every move, and these traces are much more detailed than a simple IP address.

Social Networking Sites

The rapid growth of social networking sites (SNS) like *Facebook* or *LinkedIn* has a dramatic effect on identity theft for two main reasons. First of all, they constitute the largest database in the world of personal information, quantitatively and qualitatively. All the information given to *Facebook* can escape forever from its owner's control. For example, 1.5 million *Facebook* accounts have been hacked recently *with all their associated data*, and offered for sale at the low price of 25 to 45 dollars per 1,000 contacts! [G] The terms of use often suffer of a lack of transparency, especially concerning the parameters of preservation of privacy and the ownership of content uploaded.

A second major threat of SNS concerns the registration process. Actually, SNS do not check the identity of the users and anyone can assume any name without control. These procedures could lead directly to identity theft with dire consequences for the reputation of the real persons. Anyone can create a profile with the identity of a public figure like politicians or famous artists and begin a campaign of discredit by posting hate messages. The theft of legitimate accounts is also easy in SNS and the hackers use the information contained in the profile itself to take possession of it. A last point about SNS is to know in which measure we can trust these systems for the protection of data. Most of these sites are actually free of charge for the users and their only source of income is derived from targeted advertising. The resale or the right of access to personal data for advertisers constitute an enormous information security breach.

Institutions and private companies

SNS are not the only companies from which hackers find information. The case of *WikiLeaks* has shown that institutions and governments are also vulnerable to information leakage. In most cases, users have no control over the data backup policies of institutions. Even IT companies were affected, for instance, *MySQL.com* has also been attacked in March 2011 ... by *SQL injection*! [Y] A statement has been made by Chantal Bernier, Assistant Privacy Commissioner of Canada, on 14 February 2011 to reconcile both goals of transparency of government and privacy of individuals [Z]. She recommended to take this problem into account from the outset when designing systems, and not as an afterthought. These specifications are called *Privacy-by-design*. Different levels of privacy, both internal and external, must be considered. The first one consists of checking that data are well anonymized within institutions. The second one must make it impossible to find correlations between different databases or sources. According to a study conducted by Latanya Sweeney [18], it suffices to use merely three pieces of information (ZIP code, gender and date of birth) to uniquely identify 87% of the population in the United States. For instance, she matched attributes from aggregated anonymized medical data and a voter list. As a result, she was able to identify the owners of medical records, including that of the Governor of Massachusetts. Correlation and aggregation

attacks must therefore be taken into account when designing an anonymization process.

Data flea market

Data collected by hackers may not be used directly. They are sold by batch on private forums or protected IRC channels, called *carding forum*. The price is set according to supply and demand and to the quality of information. For example, credit card numbers are negotiated from $6 to $20 for classic card up to $100 for platinum [AA]. These forums are very difficult to access because of established protection means like child pornography servers.

IV. Victims

The sociological profile of the victims is diverse. They come from all geographical regions and all socio-professional layers. Nevertheless, some features seem to discriminate against individuals and foster identity theft. First of all, the age of the people is important. Young people (20-40 years old) are over-represented among the victims of this crime; they represent about 50% of cases [12]. This observation is explained by two main facts: this population is less vigilant in the information it leaves, offline or online, in social networking sites for instance. It is the portion of the general population that uses the most Internet and online services and consequently, the probability to encounter a hacker increases statistically.

Ideally, one should make personal information harder to steal or make stolen information harder to use. However, this is very difficult since the problem of identity theft is more exacerbated within young people. They archive their own youth, as they see themselves as having an audience. *Wikipedia* is their library and *Skype* is their phone. As a result, they endanger those around them and sometimes undermine their own future!

Another factor that seems to play a significant role is the choice of the victims: the income and the financial situation of an individual is a factor, which seems logical, given that criminals seek to maximize their gain, and wealthy people use financial services more often. Another important point concerns how the victims feel after the identity theft. Actually, only half of them could say precisely how the hackers have stolen their data, which constitute a trauma or a misunderstanding. Moreover, a significant portion (5%) does not even know that the fraud from which they have been victimized is as identity theft.

Note that victims are most concerned about identity theft in stores and online, but only 25% recognize the risks at home and in institutional settings, like the office, school and government services, which hold a large amount of personal information.

Impact on victims

The first objective of a study made by [10] was to test the knowledge of the term "identity theft" among the Québec population. Their preliminary investigations have revealed that it is used by the media, police investigators and practitioners of information security to describe different practices, which has the effect of limiting its understanding among the public. To be effective, prevention campaigns should use an unambiguous language when addressing the public in order to avoid different interpretations. It is difficult to predict how long the effects of ID theft may linger. It depends on many factors, including the type of theft, whether the thief sold your information to other hackers, whether the thief is caught, and various problems related to correcting your credit report.

Moreover, it is difficult to measure a prejudice when it is not financial. "The fact that someone's cloned debit card does not incur him any liability with the issuing financial institution, makes it a lesser evil. When you go to the next level, hackers can sometimes take a second mortgage on a house without the victim knowing. Most often, people learn about it when the bank sends a bailiff to seize the house because the second mortgage was not paid", says Patry [H]. The worst level of identity theft occurs when an identity is crafted as a falsified passport. This allows hackers to move in other countries and commit crimes. "If you go, for example, to Mexico with your family and the authorities put you under arrest because someone has already gone there to commit a crime using your identity, it is extremely serious" [H].

A survey conducted by The Ponemon Institute in June 2010 showed that people who have been victims of identity theft are just equally vulnerable and ineffective in securing their personal information online. "I was surprised that those who had experienced identity theft in the past weren't taking stronger measures to protect their identity" said Larry Ponemon, founder of the Ponemon Institute [X].

Moreover, a survey conducted by *Prince Market* in May 2009, which presents measures taken by American ID theft victims to keep their personal information secure, seems to confirm this trend. 13% of respondents declared that they took no particular precaution, only 8% said they were more careful and aware. They were also only 7% of them to enroll in a credit monitoring service or a comprehensive identity theft alert program. Furthermore, the behaviour of most victims does not change fundamentally after an identity theft, which exposes them again, potentially, to this risk.

V. Hackers

The hackers often have unusual criminal profiles. Their motivations are simple. According to a survey [9], two axes can be identified: (a) The financial profits in the vast majority of cases to improve their lifestyle. (b) The reputation of public figures or firms are targeted by hacktivists mainly for political reasons, such as in the case of the publication of Sarah Palin's emails or the modification of Nicolas Sarkozy's profile on *Facebook*.

The sociological and psychological aspects are interesting to mention. Actually, the perpetrators come from all socio-professional aspects, and are distributed fairly evenly in the age pyramid. They commit their crimes most often alone (64.6%) according to [11], organized gangs of three or more are only observed in 14% of cases. This observation can probably explain another phenomenon, which is the large proportion of women in the population of hackers compared to other forms of crime (38.9%). This last fact is also correlated with another characteristic of identity theft: the non-recourse to violence in the majority of cases.

Moreover, the psychological profile of hackers is even more atypical. They often have good communication and interpersonal skills, which help them to manipulate their victims in the offline attacks. The computer screen puts a distance between them and the victims so that they do not always realize the direct consequences of their actions. The virtualization of crime gives them a feeling of power and invincibility with the police.

Highway robbery and criminal networks are also interested in profits from identity theft and use their logistical means to launder money and transform data into goods or services. These activities are far less dangerous and require less investment and organization as trafficking drugs or weapons, for example.

VI. Techniques

A. Traditional methods

Most identity fraud begins offline, intentionally or unintentionally, by different techniques. The loss or theft of items like a wallet or laptop constitutes a third of the personal information breach. Moreover, the hackers do not hesitate to use the *dumpster diving method*. It consists of sifting through garbage, looking for personal data like bank or phone statements. They can also directly steal the victim's mail to achieve information from the mail box [14].

Hackers also use more active methods to extract information from their victims by manipulating them. These techniques are called *social engineering*. Based on the abuse of trust or the naïvety of victims, it consists in extracting information by different means. Hackers ask for information without apparent danger such as date of birth during a casual conversation or use a false identity. For example, hackers can attack by phone, using the identity of a legitimate organization (bank, government) or relative (grandchild, parents) [J]. This technique is rendered even more believable through the use of *callerID spoofing*, which consists in forging any telephone number and making the called party believe that the call is originated from a legitimate source. The hackers ask for more details about the financial situation or other sensitive data. The victims believe that they are talking to a legitimate interlocutor since they have already given information such as the bank's identity. The hackers can also ask for money directly in cases of scam, after telling a story such as the *Nigerian attack* (car accident, diplomatic problem).

Some methods are subtler and use the memory of the old electronic devices. People throw out their old hard drives or smart phones without formatting them and pay no attention to the recycling process. However, they still contain the owner's data (saved passwords or scans of their documents) [K].

B. Online methods

Computers, Internet and all attached services (email, online banks) constitute new and more sophisticated methods for stealing personal data. The techniques are varied, the ingenuity and the malice of hackers know no bounds. First, they can exploit the vulnerabilities of access to the hardware installing extra modules in order to record activities. For instance, the modification of ATM (*skimming*) makes it possible to catch fingerprints of credit cards. The information is sent to the hacker by SMS or email, which then uses them for online purchases.

They can also install hardware *keyloggers* between the keyboard and the computer on public machines (cyber café) to monitor all keystrokes typed by a user. Then, they catch passwords and identifiers. Moreover, more sophisticated keylogging methods seem to be appearing. Andrea Barisani and Daniele Bianco demonstrated during the Black Hat Conference in 2009, that each pressed key causes a different vibration on the laptop. It can be determined by a simple laser pointed on the screen [5].

Spamming and *phishing* constitute other means to dupe the users; it is a kind of digital *social engineering*. They consist of unsolicited email sent from the hackers who pretend to be legitimate institutions (government, bank, insurance…) or parents. They request the users to provide personal information (credit card numbers, passwords…) or money. They can also invite the victims to visit a fake infected web site with an URL and a design close to the real one. This technique is called *typosquatting*.

Compromised software and files are also vectors of attack. Users can be infected by *malware (spyware, trojan, virus)* when they surf on corrupted websites or when they install software from non-legitimate sources (P2P, torrent). A new generation of malware and by far the most sophisticated is called *Rootkit*. Once it infects a computer, it corrupts the operating system and becomes part of its kernel, thus taking control of all the processes and putting the greatest anti-virus belly up. Interestingly enough, the earliest and most notorious user of the rootkit was no other than *Sony Corporation*. They used the rootkit technique to spy upon their customers in order to secure the digital rights of *Sony BMG* music CDs. This scandal gave new ideas to hackers and sent them running back to their drawing boards. These applications open a breach in the security of the systems and can send data and keylogging or *screenlogging* reports automatically to the hacker. Screenloggers take snapshots of the user interface regularly, or when a connection to a secured web site starts. It is very useful for the hackers, on online banks for instance, where the authentication process uses a digital keyboard.

The *SQL injection* was again the biggest application vulnerability used to steal online data in 2010, according to Open Web Application Security Project [L]. It consists of injecting SQL into the application fields in order to examine the responses of the system. This method is used to plunder databases that stores user personal information. Albert Gonzales used this technique to steal more than 130 million credit card numbers from five financial companies and stores [M].

A last set of technical means is local network attacks. The hackers can use passive methods like *sniffing* the communications between the client and the router in order to intercept information. The active attacks are more dangerous when the hacker is in a man-in-the-middle situation. He can change the default gateway, transfer all the communications or take the role of the DNS server. This last technique, called *pharming*, is used to fake web sites but with legitimate URLs. The victims

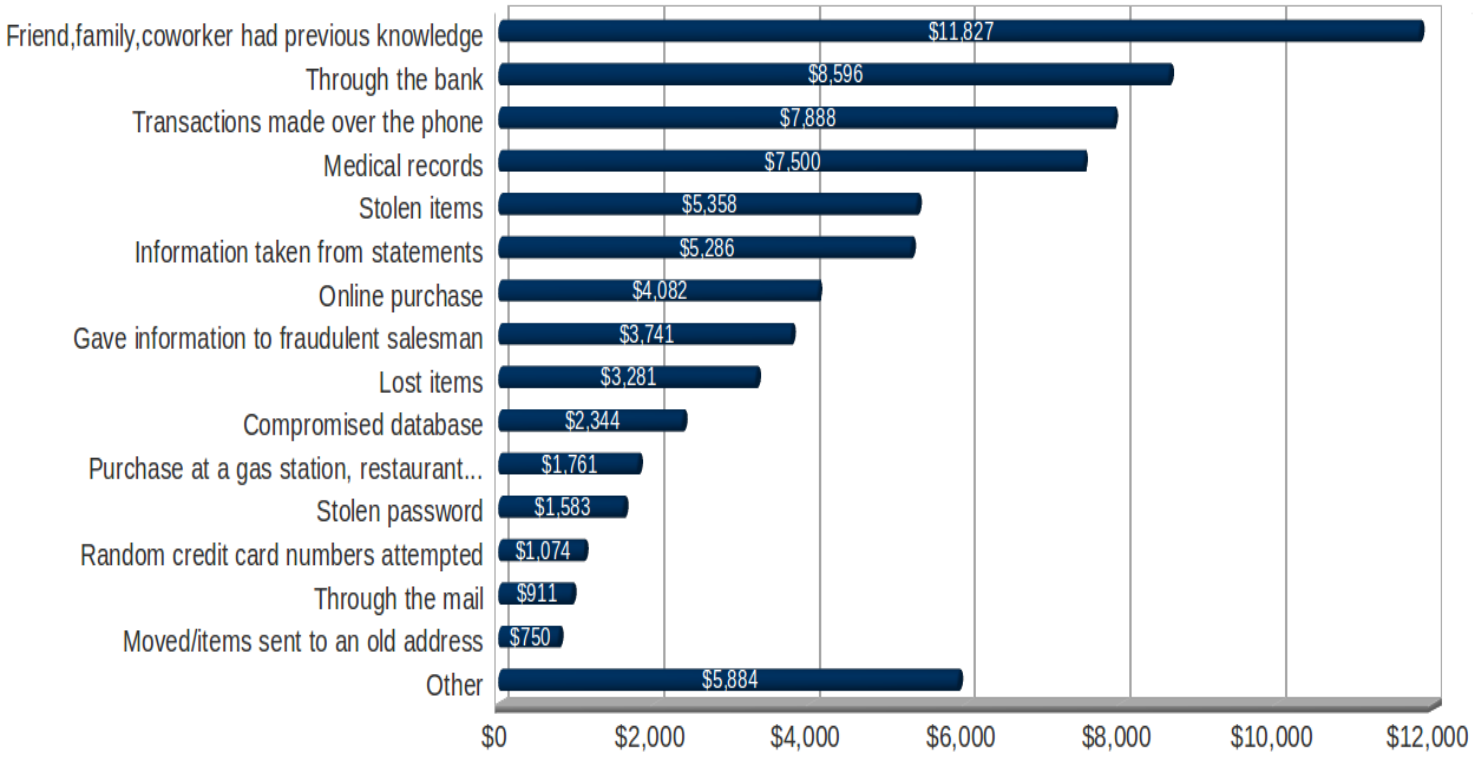

Fig. 2. Average fraud amount by means [Javelin, "2010 Identity Fraud Survey Report", February 2010]

give their identification information and other data directly to the hacker web server. A lot of open source tools are available and user-friendly to set up these kinds of attacks like *metasploit* or *ettercap*. The public WiFi access points are vulnerable and difficult to protect against these threats. Even on private networks secured by WEP or WPA keys, the theft of personal information is far to be impossible; it is just a question of time.

Hackers do not necessarily need to use system vulnerabilities or high skills to collect data. Most of the time, they can directly use system services. For instance, Herbert Thompson, a software security expert, explained in an article [BB] how he could steal an identity in less than one hour, using password recovery functionalities of mail servers and online banking sites. He knew only very little information about the victim. "Kim is a friend of my wife, so just from previous conversations I already knew her name, what state she was from, where she worked, and about how old she was. But that's about all I knew. She then told me which bank she used (although there are some pretty easy ways to find that out) and what her user name was. It turns out it was fairly predictable: her first initial + last name". The first step consisted of collecting public information from *Google*. He found Kim's blog, which was a goldmine (résumé, date of birth, hometown, old college email and *Gmail* address). He used the password recovery service of her banking site to get a new password that has been sent to her *Gmail* address. He used the same technique with her *Gmail* account in order to get a new password that he has to obtain from her College email address. "When I used the 'forgot my password' link on the college e-mail server, it asked me for some information to reset the password: home address?; home zip code?; home country? (found on her old online résumé); date of birth?". He returned on her blog and found her birth date without the year. The college email server gave him five attempts to enter the right date and he finally could have access to all the data.

VII. Legal issues of identity theft

Canada was one of the first countries to adopt legislation against identity theft with a prevention policy on one hand and a protection law on the other. The Personal Information Protection and Electronic Documents Act (PIPEDA) regulates the collection and treatment of personal data by private companies. It sets out the principles of the storage and use of data. They define what kind of information can be collected and regulate the reasons why companies would assemble, process and retain the data [N]. The adoption of the Bill S-4 in 2010 has created three offenses to penalize identity fraud: (1) possession of personal information with intent to use them for fraudulent purposes, (2) concealment of identity information, (3) possession or illegal trafficking of identity documents issued by the government containing another person's information. All these crimes are punishable by five years imprisonment, heavy fines and full compensation for the costs incurred and generated by victims. Rob Nicholson, Minister of Justice and Attorney General of Canada, said about Bill S-4, "we are not trying to stay one step ahead of hackers, we are trying to catch up to them". The institutions seem overwhelmed by the rapidity with which the methods of theft evolve.

In the United States, the legislation differs from state to state, but a federal law does exist. The Identity Theft Penalty

Enhancement Act (July 2004) condemns identity theft with two years imprisonment. However, this law is general and not targeted specifically for online theft and the new techniques [O]. Nevertheless, some states adopted stricter laws, like Texas did in September 2009 or California in January 2011. They prevent digital identity theft with the intention to commit fraudulent acts with one year in prison and/or a $10,000 fine [P].

Furthermore, the creation of the Convention on Cybercrime by the European Council made it possible to give a legislative frame to the European Union. It consists of proposals like the illegal access to a system or the threat to the integrity of data. However, this common charter lays the basis for legislation on the use of personal information for malicious purposes. In 2007, the European Commission also edited a communication called "Towards a general policy on the fight against cyber crime", which takes into account the phenomenon of identity theft. It enforces the cooperation between the countries and demands a harmonizing member state's legislation. Actually, identity theft as such is not criminalized across all members of the European Community [R].

We can point out the fact that in France, the legislative situation is also changing with the adoption of the law LOPPSI2 in February 2011. Like PIPEDA, it constitutes a legal toolbox to prevent and punish identity theft. It creates the crime of digital identity theft and condemns it with a sentence of two years imprisonment and a fine of 20,000 euros [S].

Despite government initiatives to try to fight and punish identity theft, no international law has yet been possible. This legislation would be a major step forward in the fight against this phenomenon because many attacks are launched from countries without any specific law on this subject. In addition, a common definition and classification of identity theft would improve cooperation between countries to arrest hackers.

VIII. What should vulnerable users do?

If vulnerable users want to limit the magnitude of their disclosures, reduce their exposure and minimize the probability that they will be identified, they may consider some countermeasures.

First, they should pay more attention to their waste. People should develop the habit of shredding all documents and statements that they receive from banks and other sensitive institutions. Moreover, students are more vulnerable also because of their lifestyle. According to a survey conducted by Robert Siciliano, CEO of *IdTheftSecurity*, 40% of the students leave their apartment or dorm doors unlocked and 9% share online passwords with friends [V]. Another important reflex to acquire is to use systematically the recycling industry specializing in old electronic devices and to make sure that backup media no longer contain sensitive data. More general measures of precaution must be taken such as checking bank accounts regularly in order to detect unusual expenses.

Secondly, behaviour in relation to the use of computers and networks must evolve. For instance, installing an antivirus software is a necessary but not sufficient condition to prevent infection by malware. Actually, according to Charlie Ingram (General Manager of Computer Emergency Response Team), antivirus software didn't detect malware in 80% of cases in 2006 [W]. Moreover, users must behave against phishing. For example, they should not open attachments without checking their integrity and more generally, not open an email from unknown people. Another potential danger comes from the connection to a WiFi access point. Users must take care to secure their WiFi network with a strong WPA key. In addition, they must never use sensitive online services from public wireless networks. The SNS are also dangerous because of their third party applications. For instance, *Facebook* provides an API for developers in order to create programs that interact with user data like *Farmville* [16]. However, these applications can collect without restrictions all user information and transmit them to external servers. Therefore, the users should not install any third party applications in SNS. They should also adjust their privacy setting to protect their data. Some techniques employed to navigate on the Internet have also been shown to be somewhat effective including: controlling cookies, browsing anonymously, changing passwords regularly, minimizing computer data retention intervals, protecting the network address, searching term chaffing, strong encrypting, using tools that seek data leak prevention such as *Proofpoint.com, CodegreenNetwork.com, Reconnex.com, Vericept.com, Verdasys.com,* etc.[8]

Finally, users should regularly monitor their e-reputation to ensure that a hacker does not use their identity. For instance, they can *"google"* their own name in general or specialized search engines like *123people.com*, *Pipl.com* or *iSearch.com*. Some online tools can help the users to monitor their name like *Google Alert*, which place an alert on it in order to be notified by email when it is used on the Internet.

The government and institutions must also take into account the phenomenon and work according to two levels. First, they must apply strict policies to secure citizens and user data in their own systems (*Privacy-by-design*). Secondly, they must develop prevention campaigns such as initiatives in schools (the population most affected). *Shredding day* is also organized by the Sûreté du Québec to raise awareness concerning identity theft. "The goal is to warn people against identity theft and encourage them to shred all documents that may lead to identity theft", said Geneviève Bruneau, an agent of the Sûreté du Québec.

What should fraud victims do?

Once a fraud is suspected or discovered, the victims must immediately alert various institutions. First, they should contact their banks and credit agencies to block or monitor their accounts. After that, they should complain to the police for investigation. According to [12], only 62% of victims notified a police department and a report was taken in 2010. They should file a report with an anti-fraud centre such as *phonebuster*, which recording all pertinent information on identity theft to identify trends and patterns. It is more difficult to fight against the damage to one's reputation. Actually, information on the Internet are never completely deleted. Moreover, politics of search engines like *Google* or *123people.com* are simple: they are not responsible for the results of the queries and they reflect only the content available on the web. Victims can just

contact the source of information and try to remove them. Companies also exist to take care of the e-reputation like *ReputationDefender*, a paid service that monitors the use of names on the Internet. The rehabilitation process after identity fraud is therefore long, time consuming and difficult for the victims.

IX. Conclusion

New information technologies that facilitate the communication between man and his tools have always been double-edged. For instance, the tools allow us to organize our world more quickly, but they also allow malicious persons to break into our lives with ever increasing ease. As long as computers and digital technologies are ubiquitous in our lives, often without our knowledge, the risk of attack, and specifically those related to identity theft, will increase continually.

In an Information Society, it is more important than ever to pose barriers that protect our identity and guard it against fraudulent uses. Remember that *data is never deleted* [1]. People should be aware that Search engines, free online tools, data aggregator companies, etc., are very valuable resources for hackers since they harbour very large databases that can potentially be attacked.

In conclusion, people with various e-profiles are faced with numerous privacy threats, including identity theft, but are often unaware of the danger inherent in them. Most people see computers as harmless tools and use them as such, without proper information about security and privacy issues they might encounter. Therefore, it is crucial to raise population awareness toward these issues. Indeed, in-depth knowledge of the entire technological and criminal ecosystem in which identity theft occurs is essential to the design and implementation of strategies for the prevention and control that are appropriate to the nature of the existing risks.

References

[1] C.Adams, Communication in Workshop on Computer Privacy in Electronic Commerce, Montreal, 2010.

[2] E.Aïmeur, G.Brassard, J.M.Fernandez, F.S.Mani Onana and Z.Rakowski, "Experimental Demonstration of a Hybrid Privacy-Preserving Recommender System," in Proceedings of the International Conference on Availability, Reliability, and Security (ARES-08), Barcelona, pp. 161-170, 2008 (a).

[3] E.Aïmeur, G.Brassard, J.M.Fernandez and F.S.Mani Onana, "ALAMBIC: A Privacy-Preserving Recommender System for Electronic Commerce," International Journal of Information Security, Vol. 7, no 5, pp.307-334, 2008 (b).

[4] E.Aïmeur, S.Gambs, and A.Ho, "Towards a privacy-enhanced social networking site," in Proceedings of the 5th International Conference on Availability, Reliability and Security (ARES'10), Krakow, Poland, February, 2010.

[5] A.Barisani, D.Bianco, "Sniffing keystrokes with lasers," Black Hat Conference, 2009.

[6] D.Boyd and N.Ellison, "Social network sites: definition, history, and scholarship," Journal of Computer-Mediated Communication, vol. 13 (1) article 11, 2007.

[7] Canadian Internet Policy and Public Interest Clinic, "Techniques of identity theft," 2007.

[8] G.Conti, *Googling Security*, Addison Wesley, Pearson Education Inc., 2009.

[9] H.Copes, L.Vieraitis, "Identity theft : assessing hackers' strategies and perceptions of risk," Department of Justice, 2007.

[10] B.Dupont, "Résultats du premier sondage sur le vol d'identité et la cybercriminalité au Québec," Ministère de la sécurité publique, 2008.

[11] B.Dupont, E.Aïmeur, "Les multiples facettes du vol d'identité," Revue Internationale de Criminologie et de Police Technique et Scientifique, pp. 177-194, 2010.

[12] Federal Trade Commission, "Consumer Sentinel Network Data Book," March, 2011.

[13] Freedom of Information and Privacy Association, "PIPEDA and identity theft," 2005.

[14] Organisation de Coopération et de Développement Economique, "Document exploratoire sur le vol d'identité en ligne," 2008.

[15] B.Schneier, *Schneier on Security*, Wiley, 2009.

[16] Sophos, "Security threat report 2011," 2011.

[17] S.Sproule, N.Archer, 2008, Measuring identity theft in Canada: 2008 consumer survey, MeRC working paper no. 23, McMaster University, Hamilton.

[18] L.Sweeney, "k-anonymity: a model for protecting privacy", International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002.

[A] http://www.identitytheft.com/article/palins_email_account_hacked

[B] http://www.computerweekly.com/Articles/2010/09/20/242908/Interpol-chief-admits-Facebook-ID-theft.htm

[C] http://www.francoischarron.com/-/a3I4rgv3pm/menu/

[D] http://www.oecd.org/dataoecd/35/24/40644196.pdf

[E] http://www.antifraudcentre-centreantifraude.ca/english/statistics_statistics.html

[F] http://www.freelegaladvicehelp.com/criminal-lawyer/identity-theft/8-Types-Of-Identity-Theft.html

[G] http://www.pc1news.com/news/1319/1-5-million-facebook-/accounts-for-sale.html

[H] http://www.directioninformatique.com/DI/client/fr/DirectionInformatique/Nouvelles.asp?id=58425

[I] http://www.combat-identity-theft.com/american-identity-theft-statistics.html

[J] http://www.identitytheftmanifesto.com/the-grandma-scam/

[K] http://www.techworld.com.au/article/376245/iphone_attack_reveals_passwords_six_minutes/

[L] http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[M] http://www.nowpublic.com/world/sql-injection-albert-gonzalez-steals-\130m-credit-card-numbers

[N] http://www2.parl.gc.ca/Content/LOP/LegislativeSummaries/40/2/s4-e.pdf

[O] http://www.glin.gov/view.action?glinID=183402

[P] http://www.journaldunet.com/ebusiness/le-net/usurpation-d-identite-numerique.shtml

[Q] http://www.idvictim.org/documents/375011Texas\%20Identity\%20Theft\%20Laws.pdf

[R] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

[S] http://www.net-iris.fr/veille-juridique/dossier/22348/la-loi-loppsi-ii-pour-renforcer-la-securite-interieure.php

[T] http://www.antifraudcentre-centreantifraude.ca/francais/statistics_statistics-f.html

[U] http://datalossdb.org

[V] http://robertsiciliano.com/blog/2010/09/14/college-students-at-risk-for-identity-theft-2/

[W] http://antivirus.about.com/od/virusdescriptions/a/avhype.htm

[X] http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100621005370&newsLang=en

[Y] http://www.scmagazineus.com/oracles-mysqlcom-hacked-via-sql-injection/article/199419/

[Z] http://www.priv.gc.ca/parl/2011/parl_20110214_e.cfm

[AA] http://amazingforums.com/forum1/DAGAME/forum.html

[BB] http://www.scientificamerican.com/article.cfm?id=anatomy-of-a-social-hack

[CC] http://en.wikipedia.org/wiki/ChoicePoint