Identity Theft

Radhika Soni
AIT-CSE (IS)
Chandigarh University
Mohali, India
sonyradhika07@gmail.com

Priyanka Jammwal
AIT-CSE
Chandigarh University
Mohali, India
Priyanka.e15553@cumail.in

***Abstract*—**Identity theft has become an increasingly prevalent criminal activity, since numerous people inadvertently divulge a substantial amount of personal information on a variety of online platforms, including social media, search engines, e-commerce websites, and free online tools. Users' ignorance of how easily this data may be combined, mined, and linked together presents a significant risk of identity theft in the event that it ends up in the wrong hands.

Users who participate in online activities like searching, messaging, shopping, browsing, blogging, chatting, and news sharing unintentionally build up extensive profiles about themselves as well as possibly their friends, family, coworkers, and employers. For criminals, this aggregate information is quite valuable.

Keywords—Identity theft, online vulnerability, privacy awareness.

I. INTRODUCTION

In the era of rapid Information Technology growth, particularly with the widespread use of the Internet, the speed of communication and interaction among various entities, including individuals, businesses, governments, and information systems, has significantly increased. However, this progress has given rise to a growing threat to privacy within the Information Society, often overlooked. This threat involves malicious individuals, commonly referred to as hackers, who seek to breach privacy and collect personal information for fraudulent purposes. Activities such as online browsing, shopping, banking, email communication, and gaming expose individuals to substantial privacy risks [2,3,4].

Hackers pursue various objectives, driven by motives such as amusement, curiosity, seeking recognition, causing harm, extortion, revenge, threatening organizations, or financial gain. Furthermore, hackers often feel a sense of impunity and invisibility "behind the PC," believing they can operate without being detected. A few examples of how hackers might use victims' information improperly are shown in Figure 1, which includes forging official documents with the victim's name and Social Security or Insurance Number and applying for credit cards, opening mobile phone accounts, getting loans, and opening new bank accounts.

Identity theft poses a pervasive threat, transcending boundaries between personal and professional spheres. A malefactor with access to your information can jeopardize not just your financial standing, but also your ability to secure employment or find accommodation. The ramifications extend to potential encounters with law enforcement, where your details may be disseminated to others in the illicit realm.

Illustrative instances from 2010 underscore the vulnerability of high-profile figures to identity breaches.Sarah Palin's Yahoo! email was compromised by a college student who took advantage of publicly accessible information such as her zip code, birthdate, and high school connection. Similarly, using fictitious Facebook pages, hackers targeted Ronald Noble, the Secretary General of Interpol, in an attempt to obtain private operational data.

Notably, FrancoisCharron.com unveiled a trove of counterfeit Facebook profiles impersonating Quebecois celebrities, prompting a year-long effort to eliminate these deceptive accounts.Quantifying identity theft proves challenging due to disparate data sources and calculation methodologies. Law enforcement relies on reported complaints, while researchers conduct broader population surveys.

According to the Federal Trade Commission, 4.6% of US citizens, or about 10 million people, fell victim to identity fraud in 2010, while the Ponemon Institute calculates that 1.5 million Americans were victims of medical identity theft in the same year. Highlighting the escalating trend, the Data loss database reported alarming incidents within a 15-day span in March 2011. Breaches at institutions like the University of York, Ortho Montana, and Missouri State University exposed sensitive information, reinforcing the growing menace of identity theft.

This non-technical exploration delves into identity theft, classifying its types in section 2 and outlining the array of information sought by hackers in section 3. Sections 4 and 5 examine the impacts on victims, hackers, and society. Section 6 delves into the techniques employed by hackers, while section 7 navigates the legal landscape. In conclusion, section 8 provides information on safeguarding and preventative strategies for susceptible consumers.

II. TYPES OF IDENTITY THEFT

According to the OECD, identity theft is the unlawful procurement, transfer, acquisition, or use of natural or legal personal information with the purpose of committing fraud or other crimes.Itgoes beyond financial transactions, encompassing the misuse of Social Security Numbers, online passwords, and addresses.

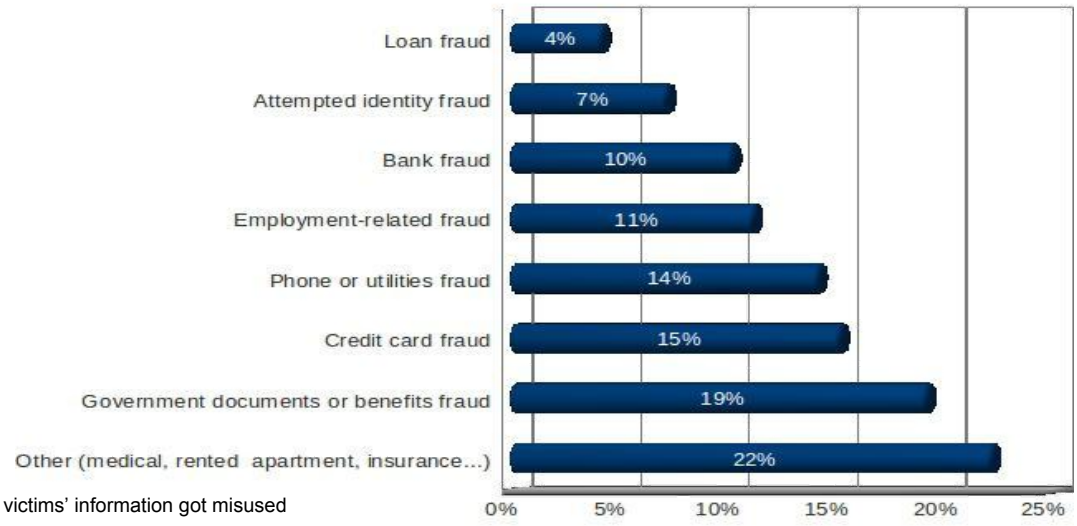

Fig. 1. How the victims' information got misused

Identity theft manifests in eight distinct forms. Financial identity theft has eroded trust in banks, leading individuals to reconsider traditional means of safeguarding their money.

People need to understand that identity theft is more than just using credit or debit cards improperly; it also includes using someone else's name, Social Security number, online passwords, and even home address without authorization.

Various forms of identity theft exist, numbering eight in total. To cite [F] in part, these include Financial identity theft, where individuals reconsider storing money outside traditional banking channels due to a lack of trust following repeated cases of financial identity theft. By exploiting someone else's insurance information to get medical care, medical identity theft occurs. When someone is discovered breaking the law and their identification is cross-checked through government databases, it may become clear that they have committed criminal identity theft. Driver's license identity theft, often resulting from lost wallets, involves hackers selling stolen driver's licenses to individuals resembling the victim. Social Security identity theft utilizes this information to evade taxes and engage in illicit activities. Synthetic identity theft is a newer form wherein the thief combines details from multiple victims to create an entirely new identity. The assumption behind child identity theft, which targets young victims and is frequently committed by a relative, is that parents won't report family members to the police. Finally, commercial identity theft happens when someone obtains a loan or credit extension under the name of a business entity.

Among these, medical identity theft is particularly alarming as its prevalence is on the rise. According to data from the Ponemon Institute, 1.5 million Americans experienced medical identity theft in 2011, with an average treatment cost of $20,663.

III. INFORMATION SOUGHT

The literature identifies three distinct stages of identity theft [17]. Initially, personal information is illicitly acquired from individuals, whether living or deceased. This information can be obtained through common methods such as theft of a handbag or wallet, or by breaching databases, even those protected by passwords, accessible to individuals with the necessary expertise and equipment. The second stage involves the illicit dissemination of stolen information, either through online illegal markets, where its value is determined by the principles of supply and demand among hackers, or through modification to create synthetic identities. The final phase encompasses the actual perpetration of fraud, with the understanding that possessing personal information of others may not be considered a legal violation in many jurisdictions [10].

An extensive range of categories are included in the hacker's search for personal information: 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.); purchasing patterns; navigational habits; lifestyle details; and sensitive data (job, medical, or criminal records). It's also possible to target biological data like blood type, genetic code, and fingerprints.

Regarding the sources of this data, Schneier [15] claims that people unintentionally leave behind data wherever they go. This extends beyond financial details, including personal emails, SMS messages, business plans, and even political affiliations. It is crucial to note that data about individuals is gathered from various sources, employing diverse methods, and by different entities [1], including governments collecting information from court records, medical histories, and mental health records.

Companies possess a vast array of personal information, including data, tax returns, and financial details. The entities you engage with, such as your cell phone provider, have precise location data, while Gmail scrutinizes emails to tailor banner ads. Google Desktop extends its reach by cataloging information from your home and office computers. Intriguingly, even companies with whom you have no direct interaction, like Acxiom, are acquiring various enterprises, ranging from direct-marketing agencies to international data firms, expanding globally. Furthermore, bankrupt companies serve as attractive targets for hackers. Cybercriminals aim to obtain unauthorised access to large databases by targeting social networks, search engines (such as Google, Yahoo!, and AOL), data aggregation companies (like the now-defunct ChoicePoint), and e-commerce behemoths (like eBay and Amazon).

Conti [8] provides an extensive account of the information that Google collects from its users, freely shared by individuals using various services like Alerts, Calendar, Catalogs, Earth, Gmail, Groups, Maps for mobile, News, Orkut, Talk, Translate, and Youtube. The disclosed data includes preferences, schedules, locations, communications, affiliations, and more [8].

Notably, search tools like 123people.com, Whozat.com, Pipl.com, Peekyou.com, PeopleSearch.net, and Peoplefinder.com are valuable resources for hackers engaged in identity theft, offering real-time searches across the web.

A variety of online and offline sources, including phone books and social networks, are compiled by social network aggregator websites like Lifehacker.com, Spokeo.com, Spoke.com, and Intelius.com. Despite potentially unintended consequences, these platforms may inadvertently provide substantial data to malicious actors.

Similarly, ChoicePoint.com [CC], which is no longer in operation, combined personal information from different public and private databases and sold it to government and commercial organisations. The company served about 100,000 clients, including law enforcement agencies, and had a database that contained more than 17 billion records of people and companies. Unfortunately, inadequate security measures led to at least one data theft incident.

Moreover, hackers exploit websites to target user databases. Blogs, for example, contain user-generated content, such as comments and discussions. It's critical that website owners know the difference between legitimate comments and client-side scripts hidden in comments. Once such malicious payloads are displayed on a website, it becomes a vulnerable point of entry.

certainly, being a participant in the network carries inherent dangers. As individuals explore additional platforms connected to Facebook, for instance,they inadvertently generate detailed traces at each interaction, surpassing the simplicity of mere IP addresses.

Networking Sites

The exponential expansion of social networking sites (SNS), such as Facebook or LinkedIn, has significantly heightened the risk of identity theft for two primary reasons. Firstly, these platforms serve as the largest repositories globally for personal information, both in terms of quantity and quality. Once information is shared with Facebook, it can permanently evade the owner's control. Recent incidents, like the hacking of 1.5 million Facebook accounts, highlight the vulnerability of personal data, with cybercriminals selling such data for as little as 25 to 45 dollars per 1,000 contacts. The terms of use often lack transparency, particularly regarding privacy preservation parameters and content ownership.

A second substantial threat from SNS revolves around the registration process. In reality, SNS lack robust identity verification, enabling users to adopt any name without scrutiny. This laxity opens the door to direct identity theft, posing severe consequences for individuals' reputations. Impersonation of public figures, such as politicians or celebrities, is easily achievable, leading to orchestrated campaigns of defamation through hate messages. Legitimate account theft is also prevalent, with hackers leveraging profile information for unauthorized access. Another critical aspect is assessing the reliability of SNS in safeguarding data. Despite being free for users, these platforms rely solely on targeted advertising for revenue, introducing significant information security risks through the sale or provision of personal data to advertisers.

Institutions and private companies

One significant risk associated with Social Networking Sites (SNS) pertains to the registration process. Notably, SNS lack stringent user identity verification, allowing individuals to adopt any name without oversight. This vulnerability poses a direct threat of identity theft, with severe repercussions for the genuine individuals' reputations. Perpetrators can create profiles impersonating public figures like politicians or renowned artists, initiating campaigns to discredit them through hate messages. SNS also facilitate the theft of legitimate accounts, as hackers exploit profile information for unauthorized access. Another concern is the reliability of SNS in safeguarding data. Many of these platforms are free for users, relying solely on targeted advertising for revenue. The sale or provision of access to personal data for advertisers represents a substantial breach in information security.

Beyond SNS, information breaches are not exclusive to private companies; institutions and governments are also susceptible. WikiLeaks highlighted the vulnerability of institutions to information leaks, emphasizing users' limited control over institutional data backup policies. Even major IT companies, such as MySQL.com, fell victim to attacks like SQL injection in March 2011. The Assistant Privacy Commissioner of Canada, Chantal Bernier, emphasised the importance of including privacy issues into system design and promoted the ideas of Privacy-by-design. These principles involve ensuring proper anonymization of data within institutions and preventing correlations across databases or sources to enhance both internal and external privacy. According to a study by Latanya Sweeney, 87% of Americans can be uniquely identified by just three pieces of information: their date of birth, gender, and ZIP code. This underscores the importance of addressing correlation and aggregation issues to protect individual privacy

Data flea market

Information obtained through hacking is not immediately utilized; instead, it is traded in bulk on exclusive forums or secure IRC channels known as carding forums. The cost is determined by market dynamics and the value of the data. For example, regular credit card numbers can be negotiated for $6 to $20, and platinum cards for as much as $100 [AA]. Accessing these forums is challenging due to robust security measures comparable to those employed by servers hosting illegal content like child pornography.

IV. Victims

The victims of identity theft display a diverse sociological profile, spanning various geographical regions and

socio-professional backgrounds. However, certain characteristics appear to contribute to the susceptibility of individuals to identity theft. Notably, age plays a crucial role, with young people (20-40 years old) representing approximately 50% of cases [12]. This is attributed to their lower vigilance in managing personal information, both offline and online, particularly on social networking sites. This age group, being the most active online, faces a statistically higher probability of encountering hackers.

Protecting personal information or making stolen data less usable is challenging, especially among the youth who consider platforms like Wikipedia and Skype as their virtual archives and communication tools. Paradoxically, their desire for self-expression and audience connection inadvertently jeopardizes their own security and that of those around them, potentially compromising their future.

Another significant factor influencing vulnerability is the financial status of victims. The income and financial situation of individuals become logical targets for criminals seeking to maximize gains, given that wealthier individuals use financial services more frequently. Additionally, the aftermath of identity theft poses challenges, as only half of the victims can precisely identify how their data was stolen, creating trauma or misunderstanding. Shockingly, a substantial portion (5%) remains unaware that they have fallen victim to identity theft.

Only 25% of victims recognise the risks in familiar settings like homes and offices, and victims express greater concern about identity theft in retail and online settings , schools, and government services, which store substantial personal information.

In addition to looking at the effects on victims, a study by [10] sought to gauge Quebecers' comprehension of what "identity theft" meant. The study found that because the phrase is used by the media, law enforcement, and information security professionals, there are different meanings of it. Effective prevention campaigns must employ clear language to minimize misunderstandings.

Measuring non-financial damages proves challenging. For instance, cloned debit cards may not incur immediate liability, but more severe cases involve thieves taking second mortgages on victims' homes without their knowledge. The most severe form of identity theft involves crafting falsified passports, enabling criminals to commit international crimes, putting innocent individuals at risk of arrest in foreign countries.

The Ponemon Institute survey in June 2010 highlighted that identity theft victims, despite their firsthand experience, exhibited vulnerability and inefficiency in securing their online information. Another survey by Prince Market in May 2009 indicated that a significant percentage of American identity theft victims took minimal precautions or did not alter their behaviors substantially after an incident, leaving them exposed to further risks.

V. Hackers

Hackers typically exhibit unconventional criminal profiles, driven by straightforward motivations. As outlined in a survey [9], these motivations can be categorized into two primary axes: (a) the pursuit of financial gains, often aiming to enhance their standard of living, and (b) hacktivists aiming to damage the reputation of public persons or corporations, primarily for political motives. Examples of this include the revelation of Sarah Palin's emails and the modification of Nicolas Sarkozy's Facebook page.

This phenomena gains an interesting dimension when its sociological and psychological components are examined. The perpetrators come from a variety of socio-professional backgrounds, with a fairly uniform distribution across age groups. According to [11], the majority (64.6%) work solo, with organized gangs of three or more only being seen in 14% of occurrences. This finding could help to explain the unusually high proportion of female hackers (38.9%), a pattern linked to the fact that most identity theft instances do not include the use of violence.

In addition, the psychological makeup of hackers is very different. Many have strong interpersonal and communication skills, which gives them the ability to control victims in offline attacks. They are insulated from the direct effects of their actions by the computer screen. Their crimes are virtual, which gives them an air of invincibility and power over law enforcement.

The prospect for large profits makes identity theft, a field more commonly linked to criminal networks and highway robberies, appealing. These organisations use their logistical prowess to transform data into goods and services and launder money. Compared to other illicit activities like drug or weapon trafficking, these activities are notable for having lower dangers, requiring less money, and requiring less organisation.

VI. Techniques

A. Traditional methods

Identity fraud frequently begins offline via a variety of methods, whether on purpose or accidentally. A considerable fraction of breaches involving personal information are caused by lost or stolen goods, such as computers or wallets. Offenders also turn to techniques like dumpster diving, in which they go through trash in an attempt to find personal information, such as phone or bank statements. Another strategy is to steal the victim's mail outright in order to obtain information from the mailbox.[14] .Hackers use more proactive measures, influencing victims with a set of tactics called social engineering. By using methods that appear innocent, this technique gathers information by taking advantage of people's trust or naivete. For example, during informal talks, hackers could ask for personal information like your date of birth or adopt a phoney identity. They may use phone calls, pretending to be a reputable company (like a bank or government) or a well-known family member (like a parent or grandchild). [J]. Caller ID spoofing makes these calls seem more credible by enabling hackers to spoof any phone number and trick the recipient into thinking it's from a reliable source. Using the previously built trust, hackers then take advantage of it to obtain further information about the victim's financial status or other private information. Sometimes, hackers may come up with claims similar to the one from Nigeria about a car accident or diplomatic issue in order to directly ask for money.Some techniques, which take advantage of the memory found in outdated electronics, are more covert. People frequently throw away their outdated hard drives or cellphones without properly formatting them, skipping the recycling procedure altogether. Still, these devices hold useful information, such as stored passwords or images of significant documents.s [K].

B. Online methods

Modern means of gaining unwanted access to personal data include computing devices, the Internet, and related services like online banking and email. The variety of techniques used demonstrates the ingenuity and malevolent purpose of hackers. They first install extra modules to record user behaviors in order to take advantage of hardware flaws. For instance, the alteration of ATMs through skimming enables the capture of credit card fingerprints, with the information transmitted to hackers via SMS or email for illicit online transactions.

Another approach involves the installation of hardware keyloggers on public machines, like cyber cafes, positioned between the keyboard and the computer to monitor and record all user keystrokes. This enables the capture of passwords and identifiers. Furthermore, more advanced keylogging methods have been developed, as Andrea Barisani and Daniele Bianco showed at the 2009 Black Hat Conference. They disclosed that a straightforward laser directed at the laptop's screen can identify the distinct vibrations that are caused by each key that is pressed.

As alternate techniques for tricking consumers, spamming and phishing are a type of digital social engineering. Hackers ask recipients of unsolicited emails to transmit sensitive information or money by pretending to be reputable organizations like banks, insurance firms, or government institutions. Another approach known as typosquatting involves luring victims to visit phony, infected websites that have designs and URLs that closely resemble real ones.

Attack vectors can also include compromised files or software. Users might become infected with malware (viruses, trojans, and spyware) by visiting tainted websites or downloading software from dubious sources like P2P or torrent sites. A more advanced type of malware called Rootkit enters a system, corrupts the kernel, and takes over all processes on the computer while eluding antivirus software. Notably, hackers were inspired by Sony Corporation's notorious use of the rootkit technology to snoop on customers.

In 2010, the Open Web Application Security Project named SQL injection as the most common application vulnerability. This technique entails inserting SQL into application fields in order to examine system answers. This technique is used to steal personal user information from databases. Using this method, Albert Gonzalez was able to obtain the credit card numbers of almost 130 million people from five different banks and retailers.

Finally, a set of technical tools is presented by local network attacks. While more dangerous active assaults use a man-in-the-middle scenario, hackers can also intercept information by passively sniffing conversations between the client and the router. Hackers have the ability to change the default gateway in these circumstances, intercept conversations, or pretend to be a DNS server. Phishing is a frequent tactic used to trick victims in which genuine URLs are utilized to create false websites.

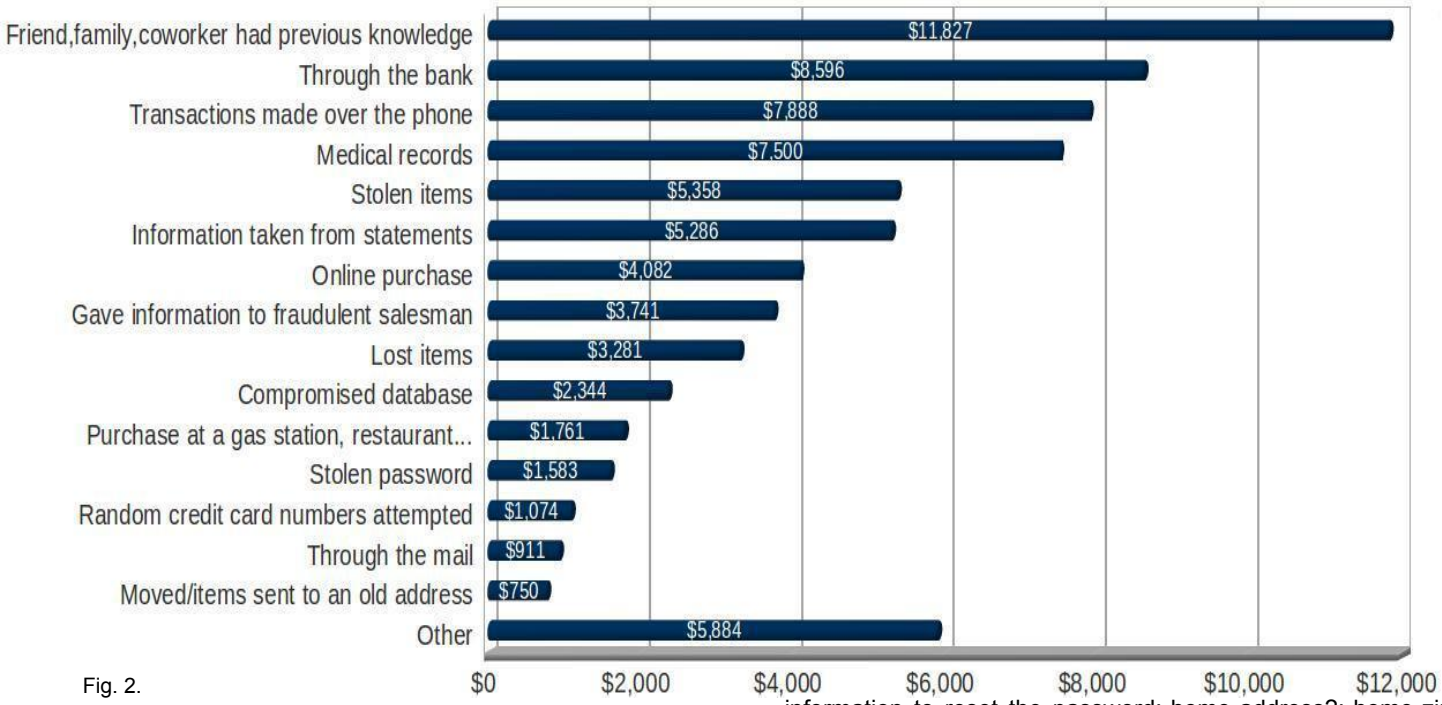

Fig. 2.

The victims voluntarily provide the hacker's web server access to their personal information, including identification details. Several open-source tools that are easy to use, including Metasploit and Ettercap, make it easier to carry out these kinds of assaults. Public WiFi connection points are vulnerable to these impending dangers and difficult to defend against. Personal data theft is a real possibility, even on supposedly secured private networks protected by WEP or WPA keys. It's just a matter of time.

Hackers don't always need to use sophisticated techniques or take advantage of system flaws in order to gather data. They can typically take advantage of current system services. For instance, software security specialist Herbert Thompson described in an article [BB] how he was able to successfully steal an identity in less than an hour. He was able to accomplish this by taking advantage of mail servers' and online banking websites' password recovery features. With less knowledge about the victim, he made calculated use of information from casual chats. Thompson recalled, "Kim is a friend of my wife, so I already knew her name, where she worked, what state she was from, and roughly how old she was from our earlier chats. 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."

Gathering public data from Google was the first step, and that's how he found Kim's blog, an absolute goldmine that included her CV, birthdate, birthplace, old college email, and Gmail address. He obtained a new password issued to her Gmail account by using the password recovery feature on her banking website. She used the same method to get a new password for her Gmail account, which she then accessed using her college email address. Thompson explained his method further, stating, "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? (discovered on her previous web résumé); birthdate? He went back to her blog and saw her birthdate (without the year). He got five chances to enter the right date on the college email system, which gave him access to a wealth of information.

VII. Legal Issues of Identity Theft

Canada took an early stance against identity theft by enacting legislation that incorporates both preventive measures and protective laws. The Personal Information Protection and Electronic Documents Act (PIPEDA) sets rules for the preservation and use of personal data and regulates how private businesses collect, handle, and use it. It outlines the kinds of data that can be collected and monitors the purposes for which businesses are allowed to acquire, use, and store this kind of information. The enactment of Bill S-4 in 2010 created three new offenses designed to punish identity fraud: the unlawful acquisition or trafficking of government-issued identity documents that contain the personal information of another person, the concealment of identity information, and the possession of personal information with fraudulent intent. These offenses include heavy fines, lengthy prison terms, and complete reimbursement of all expenses borne by the victims. Rob Nicholson, Canada's Minister of Justice and Attorney General, stressed that the goal is not just to outpace hackers but also to keep up with their changing strategies—a task made more difficult by the speed at which stealing techniques are developing. Although there is federal law in the US thanks to the Identity Theft Penalty Enhancement Act, the sanctions are broad and not especially designed for online theft and new methods. However, in order to prevent digital identity theft, some jurisdictions, like Texas and California, have passed stronger laws that come with fines and jail time.

The Convention on Cybercrime, which was established by the European Council, gave the European Union a legislative framework to address problems including unauthorised system access and data integrity risks. Legislation regarding the malicious use of personal information is based on the common charter, even if identity theft is not criminalised in every member state of the European Community. The 2007 message "Towards a General Policy on the Fight Against Cybercrime" from the European Commission addresses identity theft, emphasises international collaboration, and calls for unified laws among member states.

Moreover, France modified its legal framework in February 2011 when the LOPPSI2 law was passed. Like PIPEDA, LOPPSI2 establishes identity theft as a crime with a jail sentence and hefty fine, acting as a legal toolset to deter and prosecute identity theft..

There is presently no international law that addresses identity theft, despite government efforts to prevent it. Creating such rules would be a big step toward combating this issue, especially as many attacks come from nations with no explicit laws addressing the issue. A common definition and categorization of identity theft would also improve international collaboration in the fight against hackers.

VIII. What should vulnerable users do?

Should susceptible users wish to restrict the size of theirThose who are vulnerable to exposure may want to think about taking a few precautions if they want to limit the scope of their disclosures, lessen their susceptibility, and lessen the chance that they will be identified..

Initially, attention should be given to managing personal waste effectively. Cultivating the habit of securely disposing of all documents and statements received from financial institutions and other sensitive entities is crucial. Additionally, students, given their lifestyle, are particularly susceptible. A study conducted by IdTheftSecurity CEO Robert Siciliano found that 9% of students disclose their internet passwords with acquaintances and 40% of students leave their housing doors unlocked [V]. Using disposal services that specialise in processing outdated electronics on a regular basis is another essential practice to make sure backup media is free of sensitive data. It's also crucial to take general safeguards, such as routinely checking bank accounts for strange charges. Furthermore, behavioural patterns concerning computer and network use must undergo a transformation. Although installing antivirus software is essential, Charlie Ingram, General Manager of Computer Emergency Response Team [W], pointed out that this is not enough to stop malware attacks. Users should also be on the lookout for emails from unfamiliar sources, avoid opening attachments without first confirming their legitimacy, and exercise caution when it comes to phishing attempts. Due to the possible risks associated with WiFi connections, users should secure their networks with strong WPA keys and avoid accessing sensitive web services on public wireless networks. Social networking sites (SNS) present dangers due to third-party applications, like Facebook's API for developers creating programs like Farmville [16]. Users should avoid installing third-party applications on SNS platforms, adjust privacy settings, and adopt effective internet navigation techniques, including controlling cookies, anonymous browsing, regular password changes, minimizing data retention intervals, encrypting network addresses and using technologies like Proofpoint.com, CodegreenNetwork.com, Reconnex.com, Vericept.com, Verdasys.com, etc. to prevent data leaks. [8].

Finally, people should constantly keep an eye on their internet reputation to guard against identity theft by hackers. It can be helpful to have tools like Google Alert, which sends consumers an email whenever their name appears online. Establishing strict policies to protect citizens' and users' data within their systems (Privacy-by-design) and initiating awareness programs, particularly in schools, who are the demographic most affected, are the two main ways that government and institutions should handle this issue. According to Genevieve Bruneau, an agent of Suret ˆ e´ du Quebec, events like Shredding Day, which is hosted by Suret ˆ e du Qu ´ ebec, are meant to increase awareness about identity theft and encourage individuals to destroy papers that could be used as evidence of identity theft.

How should victims of fraud proceed?

As soon as suspicions or actual fraud cases are discovered, those who have been impacted must notify the appropriate authorities right once. They should first get in touch with their banks and credit bureaus to request that their accounts be blocked or closely watched. It is therefore imperative that you file a complaint with law enforcement so that they can conduct a full investigation. Only 62% of victims reported such incidents to the police, as shown in a research [12], and official records were only made in 2010. Furthermore, it is imperative to submit a thorough report to an anti-fraud center such as phonebuster, which scrupulously records all relevant information pertaining to identity theft and facilitates the discovery of new trends and patterns.Handling reputational damage turns out to be a more difficult task. Rumors are circulating regarding. Moreover, search engines, such as Google and 123people.com, have clear policies: they just reflect the content that is available online and take no responsibility for the results of queries. The difficult task that victims face is contacting the information providers and trying to convince them to take down the harmful content. Fortunately, companies such as ReputationDefender offer paid services that actively monitor the online usage of names, enabling consumers to take control of their online reputation. It's true that recovering from identity theft is a drawn-out procedure that necessitates victims investing a great deal of time and effort in contacting the information source and making efforts to get them deleted. Other companies do e-reputation management; one such company is ReputationDefender, a for-profit service that monitors how names are used online. Identity fraud victims must so go through a drawn-out, difficult, and time-consuming rehabilitation process.

IX. Conclusion

People need to understand that search engines, free online tools, and data aggregator organizations are attractive targets for hackers because of their large databases that could be compromised. While these tools expedite the organization of our surroundings, they also provide an increasingly accessible avenue for malicious individuals to intrude into our lives. The pervasive integration of computers and digital technologies, often without our explicit awareness, heightens the perpetual risk of various attacks, particularly those associated with identity theft. In the context of an Information Society, establishing formidable barriers becomes paramount to safeguarding our identity and shielding it from fraudulent exploitation. It's crucial to acknowledge that data, once generated, is never entirely erased. Having a thorough understanding of the full technology and criminal environment in which identity theft occurs is essential to developing and putting into practice prevention and control plans that are compatible with the nature of the threats that are now present.

In summary, individuals maintaining diverse electronic profiles confront numerous privacy threats, foremost among them being identity theft, often oblivious to the inherent dangers. Many view computers merely as benign instruments, utilizing them without comprehensive understanding of the security and privacy challenges they might confront. Consequently, there's a pressing need to heighten public awareness regarding these issues.To effectively design and implement prevention and control measures that are in line with the nature of the threats now present, one must have a thorough understanding of the full technological and criminal ecosystem in which identity theft occurs.

References

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

[2] E.A¨ımeur, 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.A¨ımeur, G.Brassard, J.M.Fernandez and F.S.Mani Onana, “ALAM-BIC: A Privacy-Preserving Recommender System for Electronic Com-merce,” International Journal of Information Security, Vol. 7, no 5, pp.307-334, 2008 (b).

[4] E.A¨ımeur, 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, “Resultats´ du premier sondage sur le vol d’identite´ et la cybercriminalite´ au Quebec,”´ Ministere` de la securit´e´ publique, 2008.

[11] B.Dupont, E.A¨ımeur, “Les multiples facettes du vol d’identite,”´ 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 Cooperation´ et de Developpement´ Economique, “Doc-ument exploratoire sur le vol d’identite´ 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”, Interna-tional Journal on Uncertainty, Fuzziness and Knowledge-based Sys-tems, 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/-/a3l4rgv3pm/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-face book-/ 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-n 130m-credit-card-numbers

[N] http://www2.parl.gc.ca/Content/LOP/LegislativeSummaries/40/2/s 4-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/375011Texasn%20Identityn %20Theftn%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