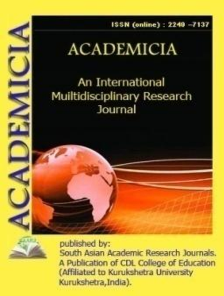
ACADEMICIA
An International Multidisciplinary Research Journal
(Double Blind Refereed & Peer Reviewed Journal)



ISSN (online) : 2249 –7137
ACADEMICIA
An International Multidisciplinary Research Journal
ACADEMICIA
published by:
South Asian Academic Research Journals.
A Publication of CDL College of Education
(Affiliated to Kurukshetra University
Kurukshetra,India).

DOI: 10.5958/2249-7137.2021.02367.3

A STUDY OF IDENTITY THEFT: INTENTIONS, CONNECTED FRAUDS, METHODS AND AVOIDANCE

Sushil Kumar*

*Faculty of Education, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, INDIA
Email id: sushilkumarmpi@gmail.com

ABSTRACT

This article provides a conceptual overview of the main crimes that result in ID fraud and millions of dollars in damages for businesses and individuals across the globe each year. The article examines the unique successful approaches for the long-term development of preventive measures that have been made available to individuals and businesses. Furthermore, the article analyzes the research and highlights the most efficient methods for individuals and businesses to protect themselves against identity theft, since victims may face a long process of repairing the harm to their reputation, credit rating, and employment. Identity theft is when someone obtains someone else's private information without their permission in order to abuse it. It will be shown how criminals use both technology-based and social engineering methods to obtain personal information. Finally, people and organizations will be given many effective preventive methods for protecting critical data and information against identity theft. Typically, criminals use human factors to get over security measures. As a result, the proposal places a strong emphasis on raising people's understanding via public and corporate training.

KEYWORDS: *Identity, Theft, Fraud, Prevention, Personal Information.*

1. INTRODUCTION

To avoid fraud as a consequence of identity theft, businesses and individuals should be careful in safeguarding their identities. How certain are they that they will not be one of the million people targeted by identity thieves in 2010? According to the Federal Trade Commission, 9.9 million Americans (22 percent higher than in 2007) were victims of identity theft in 2008, and “ID theft costs consumers approximately $50 billion annually”[1]. Despite efforts to enforce the law, the number of new identity theft victims increases on a daily basis all over the world. The preparatory stages of acquiring, holding, and trafficking in identity information for future use in current crimes such as personation, fraud, or abuse of debit card or credit card data are referred to as ID theft.

Credit card numbers, CW2 numbers (on the back of credit cards), Credit reports, Social Security (SIN) numbers, Driver's license numbers, ATM numbers, Telephone calling cards, Mortgage details, Date of birth, Passwords and PINs, Home addresses, and Phone numbers are the top twelve types of private personal information stolen by identity thieves.

ID theft is one of the main issues that costs individuals and companies billions of dollars each year all around the world. The main sources of ID theft include social and technical reasons, according to an analysis of four key variables: political, economic, social, and technology. Social engineering is a thieving method in which criminals take advantage of people's online habits, such as on Facebook, to steal personal information. This study looks at the many kinds of scams that are common as a result of identity theft. ID fraud, financial fraud, tax fraud, medical fraud, resume fraud, mortgage fraud, and organized crimes such as money laundering, terrorism, and illegal immigration are all scams that arise from ID theft. In addition, the different methods used by thieves to target people and organizations are explored. Physical and technical methods are the two main categories of techniques. Traditional methods such as mail theft and insider theft are examples of physical tactics. It is critical for managers to understand that, despite modern technology-based methods, insiders are responsible for more than 70% of ID theft.

ID theft, by definition, is typically linked with fraud and results in financial damages for victims, both people and businesses. Because victims may face a long process of clearing up the damage, such as their reputation, credit rating, and employment, it is critical to learn effective methods to safeguard individuals and businesses from ID theft. As a result, it is essential to examine the major potential variables, such as political, economic, social, and technical, and how they may promote or reduce ID theft. ID theft tactics, ID fraud, and methods of ID fraud prevention will also be addressed, since individuals and businesses need to know how to avoid fraud as a consequence of ID theft.

1.1.Analysis of Political, Economic, Social, And Technical (Pest) Factors

It is essential to scan and evaluate external or micro-environmental variables in order to take effective measures to prevent and reduce ID theft in a society. One of the major frameworks for evaluating how political, economic, social, and technical variables influence ID theft is the PEST analysis. Factors such as politics and economics, as well as identity theft ID theft has substantially increased in emerging countries due to a lack of political and economic stability, particularly in developed countries. Every year, millions of individuals from poor nations move to wealthy ones to escape poverty or political unrest[2]. More than ten million undocumented Mexicans, South and Latin Americans, and Asian immigrants reside in the United States, according to statistics. As can be observed, adverse political and economic circumstances drive individuals to immigrate illegally, resulting in identity theft and fraud.

1.2.Factors Such as Politics and Economics, as Well as Identity Theft

ID theft has substantially increased in emerging countries due to a lack of political and economic stability, particularly in developed countries. Every year, millions of individuals from poor nations move to wealthy ones to escape poverty and political unrest. The cost of illegal immigration is borne by American society in the form of identity theft, when illegal immigrants steal identities such as social security numbers or driver's licenses in order to work[3]. For example, in March 2007, the United States District Court for the Southern District of New York sentenced 20 undocumented Mexican immigrants to prison for identity theft, document fraud, and abusing Social Security numbers. As can be observed, adverse political and economic circumstances drive individuals to immigrate illegally, resulting in identity theft and fraud.

1.3.Identity Theft and Social Considerations

ID theft is influenced by the social environment and variables such as habits and social network communication. In a society, particularly in the.com sector, people's understanding of how to utilize social networks and their role in preserving privacy is critical. Companies, organizations, and individuals use a variety of security measures to safeguard their privacy, sensitive data, and personal information. Social engineering, on the other hand, is "alive and well" and "probably remains the most successful hacking method" for obtaining personal and sensitive data. Social engineering, according to Applegate, is a "methodology that enables an attacker to circumvent technological restrictions by targeting the human aspect in an organization"[4].Social engineers remain a powerful danger to people's cultural attitudes and behaviors in social networking, as communication via social networks such as Facebook, Twitter, and Skype grows. According to a study conducted by the point for credit union research and guidance in the United States, Canada, the United Kingdom, France, Germany, and Spain in 2008[5],

- I 25% of Germans and 60% of Americans have given their account passwords with a family member or acquaintance. As a consequence of this societal mindset, 3% of Germans have had their identities stolen.
- Half of all Americans use family member names, significant dates, nicknames, or their pet's name as passwords for internet accounts.
- Approximately 40% of customers in all six countries show personal information on their social media profiles, and some of them use the same information as their passwords.
- In France, more than a quarter of customers utilize their social network posted date of birth as their internet passwords.

As a result, attackers have unfettered access to this information on users' profiles. Attackers use this information to get more information without raising suspicion in preparation for a final assault, such as identity theft and fraud. A social engineer, for example, gets a financial manager's information on a social network, allowing the attacker to learn the manager's first and last name, occupation, and date of birth.

1.4.Factors Such as Technology and Identity Theft

People and institutions are threatened by technological forces. People's behavior in managing their private information, such as credit cards and social insurance numbers, has altered as new technologies, such as PDAs, mobile phones, USB, Wireless, and laptops, have entered the World Wide Web arena[6]. When individuals utilize their private information, such as banking account information, they are not completely secure no matter where they are online or at work. Fraudsters now see the Internet as a new frontier, simple to access, and a wealth of personal information from which to steal people's identities.

Mostay estimates that individuals and organizations lose approximately $40 billion per year in internet activity due to identity theft and communication fraud[7]. Furthermore, almost 80% of financial institutions use wireless technology, such as smart phones, in their operations, while only 75% of devices use mobile security. As a result, when individuals utilize new technology like Wi-Fi or online banking, it's critical that they alter their habits. One of the most common blunders is storing the online banking login and password in the browser. Individuals and technology managers must alter their attitudes and actions as a result of the new technology boom, and explore cautious measures while utilizing new technology[8]. People and individuals may be protected against identity theft by utilizing proper security measures, such as avoiding storing account information on computers, employing anti-spyware programs, and using wireless safeguards. As a result, new technological risks and their impact on identity theft vary depending on the behaviors and measures taken by people and management.

1.5.the creation of new accounts

With personal information and identification such as a victim's name, address, and social security number, fraudsters can open new bank accounts, credit accounts (credit cards, lines of credit, or loans), in-store accounts, cell phone accounts, and student loan accounts using the victim's real information; they will then change their billing address to hide their activities from the victim. In such situations, fraudsters have more time and chances to conduct fraud, and victims are usually unaware until collection agencies approach them or their credit applications are denied.

1.6.Shopping on the Internet

Fraudsters use victims' personal information and ID to buy online in a distant region, typically Africa, and ask for goods to be delivered to a trusted third party. They then request that purchases be repackaged and sent to the fraudsters. This kind of fraud became more prevalent in Canada in 2003, when an Albertan bought goods online using a stolen ID and credit card information, then requested that his order be sent to North Dakota, where it was repackaged and re-shipped to Edmonton.

1.7.Medical Espionage

When someone takes vital information or identification, such as a victim's health card, they use it to claim or receive medical services in the victim's name. One of the potential outcomes of medical fraud is deceiving health-care professionals, putting a patient's life in jeopardy. According to statistics, about 500,000 Americans have been victims of medical fraud. Although there is no data for Canada, the Ontario Ministry of Health and Long-Term Care says that medical fraud (health care fraud) is the most common result of identity theft in the province [9].

1.8.Tax Evasion

ID thieves utilize their victims' identities, such as job data or social security numbers, to file their taxes and collect their refunds. According to the United States District Court for the District of Arizona (2010), between 2005 and 2008, a gang of fraudsters submitted income tax returns using stolen IDs and received approximately $4 million in tax refunds[10].

2. DISCUSSION

Businesses and organizations must have a strategic strategy in place to safeguard critical information since they store people's identities and private information in their databases. Institutions, such as financial or governmental organizations, must ensure that red flags can be recognized by their security systems in the initial phase to have an effective and secure system. As a result, identity theft prevention programs should be made available, and they should have the following key components:

- First and foremost, reasonable rules and processes for detecting "red flags."
- Secondly, look for the red flags that have been recognized.
- Thirdly, after detecting red signals, take necessary action.
- Lastly, the preventive program should be evaluated and updated on a regular basis.

Furthermore, Collins claims that, contrary to popular belief, the bulk of ID theft occurs in the workplace rather than online. Collins claims that workers or people impersonating employees are responsible for more than 70% of ID theft in businesses; as a result, Collins advises businesses to use the following preventive measures:

- To ensure that businesses have a suitable and effective personnel selection strategy in place to ensure that honest people are hired.
- To carry out a risk assessment.
- To use an e-business risk assessment tool to spot ID theft red flags.
- To make it mandatory to shred any papers containing personal information and sensitive information about people and businesses before discarding them.
- Educate and educate staff on how to spot fraudulent applications.
- To improve the organization's ethical culture.
- To recognize and encourage workers who promote organizational honesty.

Senior Virus Research Engineer at McAfee, recommends the following preventive measures to businesses to minimize ID theft:

- Appoint someone to be in charge of the organization's security system.
- To reduce hazardous behavior such as sending and receiving email without discretion and downloading applications by providing training, outlining user duties, and documenting the information system and network's regulations.

- Create a secure network and implement secure hardware and software.
- Adopting manageable solutions for workers who are in charge of system support.
- Document all actions such as diagnosing, installing, testing, and restoring the organization's network.
- To formalize corporate network use, such as adding or removing users.
- Identify, detect, block, and report questionable online activity using preventive security technologies.
- To install dependable security systems on all terminals (servers and workstations) that link to the business network, such as anti-virus, anti-Trojan, and anti-spyware.
- To keep all security software up to date on a regular basis.
- To evaluate, update, reconfigure, and manage the company's security system.
- To disregard any free remote security system audits that may be available.
- To safeguard the organization's data backup devices.
- To avoid storing sensitive information and data on portable computers such as laptops.
- To evaluate, monitor, and manage the wireless network and devices of the company.
- Limit physical access to computers to safeguard the organization's information system.
- To reduce the danger of critical data being copied or stolen by monitoring staff turnover and job mobility.
- To manage information flow outside of the corporation's computer network, such as interviews, questionnaire answers, conference presentations, and private or public information exchanges.

3. CONCLUSION

Identity theft is becoming a significant crime all around the world, posing a danger to both individuals and businesses. Thieves, fraudsters, and criminals employ a variety of methods to acquire private information from individuals. Fraudsters' motivation, skill, and dedication are reflected in the diversity of methods they use to get personal information and the quantity of money they make. Facts indicate that thieves change their methods depending on their motivation; as a result, the costs of ID theft vary for people and organizations. As previously stated, societal and technical elements are important motivators for criminals. These two causes are intertwined and contribute to an increase in identity theft. Furthermore, fraudsters are motivated by new technology and a lack of public awareness about how to safeguard personal information.

As a result, identity thieves are expected to use new methods to acquire personal information, especially in the internet context. As a result, it is critical to improve people's understanding of how to defend oneself in online networks via media education. In terms of public education expenses, it is important to note that governments and other large businesses should see these costs as investments rather than expenditures in order to create a secure society. Banks, financial institutions, and retail shops, for example, are more susceptible than other small companies or corporations since they gather people's personal information in their databases. As a result, these institutions must have proper strategies, policies, and procedures in place to defend themselves against widespread identity theft. Security awareness, training, technical control, and an efficient information management plan should all be part of a sound defensive approach.

Identity theft by insiders is a significant issue for companies, according to statistics; thus, organizations should consider implementing a robust and effective internal control to prevent identity theft. Organizations should educate workers on the most common kind of assault, social engineering, and its effects. Managers should also be aware that poor performance and disregard for the impact of possible assaults not only results in significant financial losses, but also tarnishes the company's reputation. Individuals and organizations must recognize that they are susceptible to identity theft; as a result, implementing the most effective security system should be linked to increasing awareness of potential risks, since "knowledge is power."

REFERENCES

1. K. M. Finklea, “Identity theft: Trends and issues,” in *Identity Theft: Trends and Prevention Efforts*, 2012, pp. 1–38.
2. O. Muniz, W. Li, and Y. Schleicher, “Migration Conceptual Framework: Why do people move to work in another place or country?,” *AAG Center for Global Geography Education*, 2016. .
3. C. Gerken, *Model immigrants and undesirable aliens: The cost of immigration reform in the 1990s*. 2013.
4. S. D. Applegate, “Social engineering: Hacking the wetware!,” *Inf. Secur. J.*, vol. 18, no. 1, pp. 40–46, 2009, doi: 10.1080/19393550802623214.
5. M. Alexander, “Methods for Understanding and Reducing Social Engineering Attacks,” *SANS Read. Room*, pp. 1–79, 2016.
6. T. Kwon and H. Moon, “Multi-modal techniques for identity theft prevention,” in *Lecture Notes in Computer Science*, 2005, vol. 3597, pp. 291–300, doi: 10.1007/11527725_30.
7. A. Litan, “Phishing attack victims likely targets for identity theft,” *Gart. First Tak. FT-22*, no. May, pp. 4–6, 2004.
8. N. A. Manap, A. A. Rahim, and H. Taji, “Cyberspace identity theft: The conceptual framework,” *Mediterr. J. Soc. Sci.*, vol. 6, no. 4S3, pp. 595–605, 2015, doi: 10.5901/mjss.2015.v6n4s3p595.
9. Z. Geradts, “Identity Theft,” in *Encyclopedia of Forensic Sciences: Second Edition*, 2013, pp. 419–422.
10. K. Veena and K. Meena, “Performance evaluation of cyber criminal detection techniques,” *Int. J. Simul. Syst. Sci. Technol.*, vol. 19, no. 4, p. 4.1-4.11, 2018, doi: 10.5013/IJSSST.a.19.04.04.