International Journal of Engineering Research
Volume No.6, Issue No.9, pp : 422-424
ISSN:2319-6890 (online),2347-5013(print)
1 Sept. 2017

Identity Theft

Matthew N. O. Sadiku, Mahamadou Tembely, Sarhan M. Musa
Roy G. Perry College of Engineering Prairie View A&M University Prairie View, TX 77446
Email: sadiku@ieee.org, tembely_madou@yahoo.fr, smmusa@pvamu.edu

Abstract: Identity theft (IT) occurs when someone uses your sensitive personal information without your consent. The personal information may include name, date of birth, address, social security number, mother's maiden name, bank account number, credit card number, phone number, driver's license number, state ID number, or email password. Identity theft has become a major area of public concern and a growing problem throughout the world. No one is safe from becoming its victim. The paper provides a brief introduction to IT.

Keywords: Identity theft, identity fraud, Internet fraud, cybercrime

I. Introduction

Identity theft, fraud, and abuse are problems affecting all segments of our society. Identity theft can be financial, medical, and character-related. If we cannot trust banks, healthcare providers, colleges, and government entities to protect our privacy, who can we trust [1]?

Identity theft (IT) refers to fraud that involves in getting personal gain by pretending to be someone else. It is a serious white-collar crime that affects lives and society worldwide. It is a behavior that threatens the growth and development of economies worldwide and has been viewed as the crime of the new millennium. It is a criminal modern activity that depends on digital culture and networked computing.

Identity theft occurs when a person uses another person's personal information such as name, date of birth, social security number, insurance information, or credit card number to gain a financial advantage or commit fraud. The criminal can use the personal information for criminal activities such fraudulent use of telephone, fraudulent withdrawals from bank accounts, false applications for credit cards, or hacking into networks without permission. Although the victim of ID theft may not find out months after the fact, the victim is responsible for what the thief does while using the personal information.

Identity theft is a criminal activity or fraud in which the victim and offender seldom meet face-to-face. Criminologists have recognized that technological changes can create new opportunities for identity theft victimization. The Internet has created new opportunities and a new conducive environment in which IT can take place [2]. This is why IT has been regarded by some as the quintessential crime of the information age.

An identity thief could be an individual criminal or a terrorist. He may not be faceless strangers, but often someone the victim knows, such as a relative, family friend, or colleague. Identity thieves can destroy personal credit and potentially involve litigation that may take years to correct. As shown in Figure 1, there are several techniques used in stealing someone's identity [3]. Those ways include mail theft, phishing (or web spoofing), hacking, and social engineering. The most disastrous consequence of identity theft is not really the loss of money, but rather the loss of credit, reputation, and erroneous information that is difficult to restore.

According to the Federal Trade Commission (FTC), nine million new cases of identity theft are reported each year and identity theft was the number one source of consumer complaints. Identity theft in the US has resulted in direct losses totaling hundreds of billions of dollars exerted on individual victims, businesses, and governments over the past few years. Issues of IT have become a priority for FTC and the Departments of Justice and Treasury. It is a threat to both the US economy as well as to global financial markets [4].

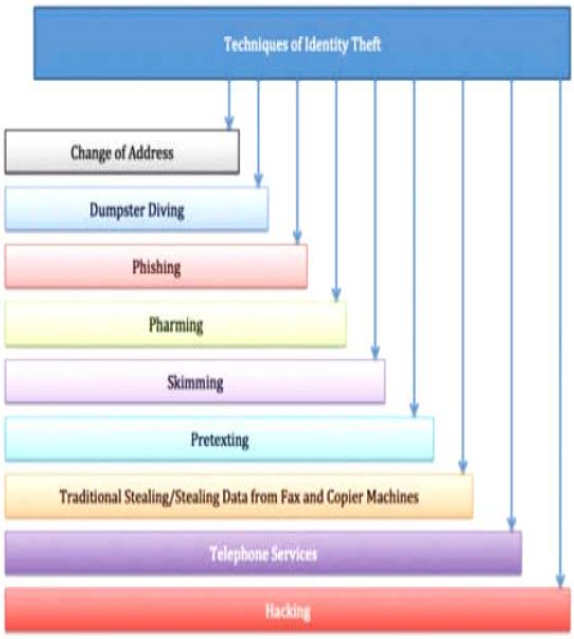

Figure 1 Techniques used to commit identity theft related crimes [3].

II. Categories Of IT

The identity thief masquerades or impersonates someone else in order to conceal their own real identity. Identity theft can be grouped into four categories [5]:

- *Financial identity theft*: using another's identity to obtain goods and services, e.g. bank fraud. The imposter uses personal information, typically a social security number, to establish credit in the victim's name.

• *Criminal identity theft*: posing as another when apprehended for a crime. The imposter gives another person's personal information to law enforcement officials.

• *Identity cloning*: using another's information to assume his or her identity in daily life. The imposter uses personal information to live and works as the victim.

• *Business/corporate identity theft*: using another's business name to obtain credit.

A corporate identity is established by the presence of websites, databases, e-mail addresses, the registration of domain names, etc. Corporate identity theft occurs through data breach disclosure or stealing of personal data of a compnay by an employee.

Other forms of IT include medical IT which is a crime involving patients and healthcare providers and character IT which is giving the personal information of someone else.

III. Recovering From IT

To recover from identity theft, the following four steps should be taken [6]. First, victims should contact the police and file a report. Police reports are vital when trying to prove victimization to credit bureaus, account providers, and government authorities. An Identity Theft Affidavit should also be filled out. Second, victims should contact the three major credit bureaus (Equifax, Experian, and TransUnion) to acquire copies of their credit reports to examine for discrepancies. Third, victims should close any accounts where they suspect involve identity theft activity has occurred. The victims may be asked to change the PIN and passwords immediately. Finally, they should log complaint to government authorities. You can call FTC Identity Theft Hotline: (877) IDTHEFT.

IV. Combating IT

Since IT is insidious and pervasive, measures to combat it must be considered. Combating identity requires collaboration from all involved stakeholders, through efforts in government, education, technology development, security management, and law enforcement. Federal and state governments have taken an initiative to pass legislation to prevent and to help those that fall victim to the crime. For example, in 1999, the Financial Modernization Act mandated financial institutions pay better attention to customers' personal information. An important federal legislation focusing on the crime of IT is the Identity Theft Penalty Enhancement Act of 2004. As the crime of identity theft grows, the government has moved from simple
prohibition to prevention [7].

Recently, identity theft protection services have become available in many nations. These services (or insurance) aim to protect the individuals from identity theft. They can detect a wide range of threats and alert the customer by phone, email, and text of the suspicious activity. For example,. *Equifax*, one of the three largest consumer reporting agencies, offers identity theft insurance for a monthly fee.

There are also identity theft prevention technologies such as biometrics and smart cards. Biometrics (retina scans, photos, height, weight, eye color, DNA, etc.) is a form of identification that is not easily replicated by identity thieves. Smart cards can store biometric information to deliver secure and accurate identity verification [8].

The following tips will help minimize the risk of identity theft [9]:

- Pay attention to your billing cycles....
- Guard your mail from theft....
- Do not give out personal information....
- Keep items with personal information in a safe place....
- Give your social security number (SSN) only when absolutely necessary....
- Don't carry your SSN card; leave it in a secure place....
- Order a copy of your credit report from each of the three major credit reporting agencies every year …

If consumers take these preventative measures, their chance of becoming an IT victim will be minimized.

V. Conclusion

The proliferation of the online business transaction has led to a large number of incidents of identity theft. Identity theft is an important issue in all areas of life and is an insidious crime. It has become a major area of public concern and a growing problem throughout the world. No one is immune from the risk of identity theft victimization.

We need to educate individuals and organizations about the risks of identity theft and the countermeasures available. Individuals should be aware of what they can do to prevent their personal information from going into the wrong hands. Society should understand all realms of identity theft, how they occur, and what could be done should we fall victim to this crime. The wide variety of information sources available on the Internet needs some form of protection. Research on IT must continue if the rise in identity theft incidence is to be abated.

References

i. H. Berghel, "Identity theft and financial fraud: some strangeness in the proportions," Computer, January 2012, pp.86-89.

ii. B. W. Reyns, " Online routines and identity theft victimization: further expanding routine activity theory beyond direct-contact offenses," Journal of Research in Crime and Delinquency, vol. 50, no. 2, 2013, pp. 216-238.

iii. A. Awasthi, "Reducing identity theft using one-time passwords and SMS," The EDP Audit, Control, and Security Newsletter (EDPACS), vol. 52, no. 5, 2015, pp. 9-19.

iv. N. L. Piquero , M. A. Cohen, and A. R. Piquero, "How much is the public willing to pay to be protected from identity theft?" Justice Quarterly, vol. 28, no. 3, 2011, pp. 437-459.

v. G. Kołaczek, "An approach to identity theft detection using social network analysis," Proceedings of the First Asian Conference on Intelligent Information and Database Systems, 2009, pp. 78-81.

vi. J. Whitson, "Identity theft and the challenges of caring for your virtual self," Interactions, vol. 16, no. 2, March/April 2009, pp. 41-45.

vii. R. Haygood and R. Hensley, "Preventing identity theft: new legal obligations for businesses," Employment Relations Today, Autumn 2006, pp.71-83.

ISSN:2319-6890 (online),2347-5013(print)
1 Sept. 2017

viii. W. I. Wang, Y. Yuan, and N. Archer, "A contextual framework for combating identity theft," IEEE Security & Privacy, March/April 2006, pp. 30-38.

*a. D. **J.** Solove, "Identity theft, privacy, and the architecture of vulnerability," Hastings Law Journal, vol. 54, 2003, pp. 1227-1276.*

About the authors

Matthew N.O. Sadiku is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.

Mahamadou Tembely is a Ph.D student at Prairie View A&M University, Texas. He received the 2014 Outstanding MS Graduated Student award for the department of electrical and computer engineering. He is the author of several papers.

Sarhan M. Musa is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.