Chapter 14

Fraud and Identity Theft Issues

Ranaganayakulu Dhanalakshmi
Anna University, India

Chenniappan Chellappan
Anna University, India

ABSTRACT

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically for economic gain. In spite of the different possible attacks discussed in later chapters, this chapter can focus on phishing attacks—a form of indirect attacks—such as an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. Phishing attacks use ‘spoofed’ e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, et cetera. The vulnerabilities on various phishing methods such as domain name spoofing, URL obfuscation, deceptive e-mails, spoofed DNS and IP addresses, and cross site scripting are analyzed, and the chapter concludes that an integrated approach is required to mitigate phishing attacks.

1. INTRODUCTION

Identity theft is one of the major upcoming threats in cybercrime which defines as an unlawful activity where the identity of an existing person is used as a target without that person’s consent. It is a specific form of identity fraud. Identity fraud is a fraud committed with identity as a target. Identity Theft and Identity Fraud can be brought under the terminology of “Identity related crime” which concerns all punishable activities that have identity as a target or a principal tool. Identity
Fraud and Identity Theft Issues

Theft/fraud in the financial system affects four main kinds of victims, essentially governments, private companies detaining large amounts of data, financial services providers and customers (whether businesses or natural persons) and the consequences for them vary. There are obviously direct financial losses, e.g. the amounts directly extracted by criminals from the accounts etc, but also indirect costs for businesses, governments and consumers in spoiling their names.

A person’s identity is very essential, concrete, and valid in a real world and is supported by legal documents. In the online world, however, a person’s identity is less tangible. Some digital data, such as passwords, account names, and logins, may not be considered elements of a person’s legal identity. Such data can be made valid in identifying and providing access to other private data.

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) defines Identity theft as

“A fraud committed using the identifying information of another person, subject to such further definition as the FTC [Federal Trade Commission] may prescribe, by regulation.” Pursuant to FACTA, the FTC has recently proposed a more specific definition of identity theft that describes what is meant by “identifying information”:

1. The term ‘identity theft’ means a fraud committed or attempted using the identifying information of another person without lawful authority. Identifying information may be
   a. Name, SSN (Social Security Number), DOB (date of birth), Government-issued driver’s license or identification number, Passport number, PAN number (Tax Payer identification number).
   b. Unique biometric data, such as fingerprint, voice print, retina or iris image representation

2. METHODS OF IDENTITY THEFT

The following overview gives the most important techniques used to obtain identity-related information. Methods of Identity theft can be classified as follows (see also Table 1).

2.1 Traditional Physical Methods

- Direct Access to information - By persons who gain trust over the individuals.
- Dumpster Diving – obtaining information from trash bins
- Theft of physical objects like purse/wallet, cell phones, computers having high source of information
- Shoulder surfing – Persons who obtain the identity data when accessing ATMs.
- Mail theft – obtaining from mail boxes
- Skimming – Magnetic strip duplication

Top-Ten IT Issues, 2010. As per a recent survey by EDUCASE, the top ten IT issues identified are:

1. Funding IT
2. Administrative/ERP/Information Systems
3. Security
4. Teaching and Learning with Technology
5. Identity/Access Management
6. a) DisasterRecovery/BusinessContinuity(tie)
7. b) Governance, Organization, and Leadership(tie)
8. Agility, Adaptability, and Responsiveness
9. Learning Management Systems
10. Strategic Planning
11. Infrastructure/Cyber infrastructure

Hence identity and access management is very crucial in this fast evolving world which finds more importance.
Related Content

Critical Evaluation of RFID Security Protocols
www.igi-global.com/article/critical-evaluation-rfid-security-protocols/72724?camid=4v1a

Memory-Based Antiforensic Tools and Techniques
www.igi-global.com/article/memory-based-antiforensic-tools-techniques/2478?camid=4v1a

Mutual Correlation-Based Anonymization for Privacy Preserving Medical Data Publishing
www.igi-global.com/chapter/mutual-correlation-based-anonymization-for-privacy-preserving-medical-data-publishing/203394?camid=4v1a

Improving Reliability and Reducing Risk by Separation
www.igi-global.com/article/improving-reliability-and-reducing-risk-by-separation/188680?camid=4v1a