A Survey on Fraud and ID Thefts in Cyber Crime

[1] Manish Kumar Jha, [2] Dr.Surendra Yadav, [3] Rishindra, [4] Shashi Ranjan

[1, 2] Computer Science & Engineering Department, MACERC (SIRSI Road)
Jaipur, Rajasthan ,302012, India

[3, 4] Computer Science & Engineering Department, SGVU (Research Scholar)
Jaipur, Rajasthan ,302012, 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. This article is an attempt to provide a glimpse on fraud & id theft. Several traditional crime are now being helped or encourage through the use of computer and network, and before they never imagined the misdeeds and showed due to the amazing skills of information systems. Then Cybercrime are calling for law enforcement services, In generally the criminal investigators, are to adjust for a growing number of their effort to succesfully identification, learn, and care in achieving success of developer.

Keywords - *Id thefts, Cybercrime, Criminal Investigators.*

1. Introduction

The application of Computer use over the Internet is increasing on account of lower holding costs of the computer and their connectivity, as well as it is faster and easier accessibility for the user. Such as –In another way both of commercial transaction and personal , one that is highly dependent on the interactions across the computers and automated agents, instead of against each other that increases the distance and provides the anonymity, which is another avenue for the crimes of perpetuate. "Computer Crime" includes the crimes committed against the PC the materials contained in it as a software and data, and its use as an processing tool. These include :-hacking, denial of service attacks, unauthorized use of services and cyber vandalism. "Cyber Crime" describes criminal activities committed via the use of electronic means of communication.

Various Acts Dealing With Frauds & Id Theft In India

1.1 Concept of CYBER FRAUD:

Information Technology solutions have paved a way to a new world of internet, business networking and e-banking, budding as a solution to reduce costs, change the sophisticated economic affairs to more easier, speedy, efficient, and time saving method of transactions. Internet has emerged as a blessing for the present pace of life but at the same time also resulted in various threats to the consumers and other institutions for which it's proved to be most beneficial. Various criminals like hackers, crackers have been able to pave their way to interfere with the internet accounts through various techniques like hacking the Domain Name Server (DNS), Internet Provider's (IP) address, spoofing, phishing, internet phishing etc. This seminar contributes an understanding of the effects of negative use of Information technology, and how far the present law in India is successful in dealing with the issue, and what way is the legal structure lagging to curb the crime. Possible changes needed in the system and the ways to combat cyber terrorism having safe and trustworthy transactions.

1.2 Fundamental of Cyber Fraud

Cyber criminals usually use the computer as a tool, target, or both for their unlawful act either to gain information which can result in heavy loss/damage to the owner of that intangible sensitive information. Internet is one of the means by which the offenders can gain such price sensitive information of companies, firms, individuals, banks, intellectual property crimes, selling illegal articles, pornography etc. this is done through many methods such as phishing, spoofing, pharming, wire transfer etc. and use it to their own advantage without the consent of the individual. Many banks, financial institutions, investment houses, brokering firms etc. are being victimized and threatened by the cyber terrorists to pay.

1.3 Types Of Fraud

Hacker is computer expert who uses his knowledge to gain unauthorized access to the computer network. He's not any person who intends to break through the system but

also includes one who has no intent to damage the system but intends to learn more by using one's computer. Crackers on other hand use the information cause disruption to the network for personal and political motives. Hacking by an insider or an employee is quite prominent in present date. There are various methods used by hackers to gain unauthorized access to the computers apart from use of viruses like Trojans and worms etc.

A) Online Fraud: The net is a boon for people to conduct business effectively, very quickly. It saves businesses a lot of time, money and resources. Unfortunately, the net is also an open invitation to seamstress and fraudsters and online frauds are becoming increasingly rampant.
User receives emails from anonymous sources which may contain:

A) Offers on purchasing an item
B) Asking for investing money
C) Some malicious links
D) Prize winning or Lottery
E) winning mails etc.

B) Phishing: By using e-mail messages which completely resembles the original mail messages of customers, hackers can ask for verification of certain information, like account numbers or passwords etc. here customer might not have knowledge that the e-mail messages are deceiving and would fail to identify the originality of the messages, this results in huge financial loss when the hackers use that information for fraudulent acts like withdrawing money from customers account without him having knowledge of it.

C) Spoofing: This is carried on by use of deceiving Websites or e-mails. These sources mimic the original websites so well by use of logos, names, graphics and even the code of real bank's site.

D) Phone Phishing: Is done by use of in-voice messages by the hackers where the customers are asked to reveal their account identification, and passwords to file a complaint for any problems regarding their accounts with banks etc.

E) Click Fraud: It occurs on the internet in pay per check online advertising. It also known as link fraud because links aren't actually what they seem.

F) DENIAL OF SERVICE: It refers to unauthorized or illegal data alteration. Data alteration may occur before and during data input or before output.

G) NIGERIAN 419 FRAUD: It is a confidence trick in which the target is persuaded to advance relatively small sums of money in the hope of realizing a much larger gain. "419" comes from the section of the Nigerian Penal Code outlawing fraudulent criminal activities by its citizens.

1.4 Identity Theft

A form of stealing someone's identity to gain access to resources or obtain credit and other benefits in that person's name (victim). Identity theft can take place whether the fraud victim is alive or deceased.

Identity Theft Types:

A) Cloning & Concealment
B) Criminal Identity Theft
C) Synthetic Identity Theft
D) Medical Identity Theft
E) Financial Identity Theft

1.5 Data Protection

Information stored on the owner of the computer would be his property and must be protected there are many ways such information can be misused by ways like 'unauthorized access, computer viruses, data typing, modification erasures etc. Legislators had been constantly confronted with problem in balancing the right of the individuals on the computer information and other people's claim to be allowed access to information under Human Rights. The first enactment in this regard was Data Protection Act by Germany in the year 1970. This was widely accepted by the world and also contributed to the Information Technology Act.

1.6 Prevention

1.6.1 General Guidelines on Cyber Safety

- Do not give out identifying information such as your name, home address, or telephone number in a chat room. Even vital details like age, gender should never be divulged to anyone.
- Do not send your photograph to any one on the net unless you know the person well enough.
- Do not respond to messages or bulletin board items that are obscene, belligerent or threatening.
- Never arrange a face-to-face meeting with someone who you have just 'met' on the Internet. In case you have to meet this person, make sure you have someone with you for the meeting. And inform someone of the person and place you will be going to. Remember, people online are not always who they seem to be.

1.6.2 Email Safety

If you ever get an email containing an embedded link, and a request for you to enter secret details, treat it as suspicious. Do not input any sensitive information that might help provide access to your bank accounts, even if the page appears legitimate. No reputable company ever sends emails of this type.

1.6.3 Virus Warnings

Virus warnings are a very common occurrence in the mail box. While you shouldn't take these warnings lightly, a lot of times, such warnings are hoaxes and will do moe harm than good. Always check the story out by visiting an anti-virus site such as McAfee, Sophos or Symantec before taking any action, including forwarding them to friends and colleagues.

1.6.4 For Home PC Users

Here are some extremely important guidelines for home computer owners.

1. Use the latest version of a good anti-virus software package that allows updating from the Internet.
2. Use the latest version of the operating system, web browsers and e-mail programs.
3. Don't open e-mail attachments unless you know the source. Attachments, especially executables (those having .exe extension) can be dangerous.
4. Confirm the site you are doing business with. Secure yourself against "Web-Spoofing". Do not go to websites from email links.
5. Create passwords containing at least 8 digits. They should not be dictionary words. They should combine upper and lower case characters.
6. Use different passwords for different websites.
7. Send credit card information only to secure sites.
8. Use a security program that gives you control over "Cookies" that send information back to websites. Letting all cookies in without monitoring them could be risky.
9. Use firewall.

2. Cyber Law

India has enacted the first I.T.Act, 2000 based on the UNCIRAL model recommended by the general assembly of the United Nations. Chapter XI of this Act deals with offences/crimes along with certain other provisions scattered in this Acts .The various offences which are provided under this chapter are shown in the following table: -

2.1 Offence Section under IT Act

2.1.1Tampering with Computer source documents Sec.65
2.1.2Hacking with Computer systems, Data alteration Sec.66
2.1.3 Publishing obscene information Sec.67
2.1.4 Un-authorised access to protected system Sec.70
2.1.5Breach of Confidentiality and Privacy Sec.72
2.1.6Publishing false digital signature certificates Sec.73

2.2 Computer Related Crimes Covered under IPC and Special Laws Offence Section

- Sending threatening messages by email Sec 503 IPC
- Sending defamatory messages by email Sec 499 IPC
- Forgery of electronic records Sec 463 IPC
- Bogus websites, cyber frauds Sec 420 IPC

3. Conclusion

The modern thief can steal more with a computer than with a gun.Tomorrow's terrorists may be able to do more damage with a keyboard than with a bomb.

References

[1] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
[2] Internet Security Systems. March-2005.
[3] Computer fraud charges in New York. May 2011. Bukh Law Firm, PC - 14 Wall St, New York NY 10005 - (212) 729-1632. New York computer fraud lawyer
[4] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace*, ABC-CLIO, 2010,
[5] A to Z of cyber crime by Aaushi Shah
[6] www.cyberlawsindia.net
[7] www.google.com