CHAPTER – II

IDENTITY THEFT; SOCIAL ENGINEERING AND CYBER CRIMES
CHAPTER - II

IDENTITY THEFT; SOCIAL ENGINEERING and CYBER CRIMES

2.1 Identity Theft

2.1.1 What is Identity?

 Mostly identity is thought of as physical being; body. Millennia ago, the only source to identify an individual human is by means of his extraneous visual aspect and verifying whether it matches with some genial image previously stored and if it was sufficiently close enough, the person is accepted as authentic, or else, he was considered to be an impostor.

 Animals use other means of identification: smell. Human being expanded their repertory as their mode of communication developed: sound became a means of identification. As society grew in complexity, new means to identify people were found. As the interests sprang up, in order to accurately recognise an individual for security or financial purposes, ways of impersonating and recognising became more advanced.

 Identity attributes might be measured into three types:

• Physical Attributes
  
  ▪ By way of Appearance (Face, Gender, Stature)
  ▪ By means of Behaviour (Personality traits, Posture, Gait, e.g. way of typing)
  ▪ Biology (Voice recognition, DNA, Fingerprints, Retina or retinal patterns)
  ▪ Augmentation (Personal Records, RFID)

• Assigned Attributes
  
  ▪ Name, Address
  ▪ Identifying number (Driving license no.)
  ▪ Ad hoc Account No. (Financial credentials like Credit cards, Bank account)
  ▪ Computer linked (Passwords, Crypto logic Keys)
• Abstract Attributes

What a person knows (Mother’s maiden name, Company of First T.V set, Refrigerator).

Virtually all of the above mentioned attributes are used at some point in order to recognise a person, with exclusion of attributes which are more tedious to draw out such as DNA or iris, retina forms. The “assigned attributes” needs related proofs (Birth Certificate, Passport, Credit cards, Identity Card). The assigned attributes can more easily be transported to another person than the physical attributes. Due to this Identity theft becomes an easier task for criminals.

2.1.2 Why Steal an Identity?

A criminal may wish to presume another person’s identity due to many common motivations, like gaining control to that person’s assets like financial, physical properties, etc. and also to violate physical security. These are impermanent assumptions of an individual’s identity, but some criminals desire to permanently alter identity to illicitly migrate to other nation and a hunted criminal trying to avoid arrest.

Due to the outgrowth of internet, Information is becoming available freely and rapidly. By using a variety of freely-available online databases, an individual’s PII could be accurately obtained. Even though this was possible even before the existence of Internet, the criminals work is made easy by the network’s presence. As the corporate databases, store an individual’s entire personal profile, which are more enough to effectively assume that person’s identity, information security has emerged to be more and more important as these corporations seek to avoid the lawsuits and bad publicity resulting from their data bases being hacked and customer information stolen (Griffith et al., 2015).

2.1.3 The Crime of Identity Theft

Identity theft is the act of one person assuming the identity of another by means of simulating or acquiring identifying instruments, without the consent of the legitimate owner. The attacker attempts to become another individual virtually in all aspects. It is a crime in which someone wrongfully obtains another person’s personal information and then uses that information to commit fraud. The circumstance in which someone
knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law or that constitutes a felony under any applicable State or local law (Identity Theft and Assumption Deterrence Act, 1998).

The digital society, where details about a person have been made more approachable, is much concerned about Identity Theft. This menace has grown in present days due to the development in the global computer networks, where information in digital form can be collected through enormous avenues and can be easily obtained. The www is important tool for criminals getting to cyberspace. Identity theft is responsible for the loss of billions of dollars worldwide, and a significant component of modern identity theft is online fraud. However, technical expertise is a known mitigating factor in computer crime.

In the past, computer crimes were small, local problem perpetrated by the few, petty thieves. However, in recent years it has revolutionized to become a more globalized problem with massive economic costs. Attacks against people’s personal and confidential information are on the rise and every citizen is at risk. It is essential that individuals take a proactive position in securing their personal information and defending themselves against these serious crimes (DataLoss DB, 2013).

Eighty-one percent of respondents cited phishing emails as a significant concern relating to the security of their personal and financial information when conducting online transactions (Identity Theft Resource, 2015).

2.1.4 Identity Theft in a Computer Context

The cyber criminals use Internet as a new and powerful mean of advantage available to carry out nameless, spamming, and crooked impersonation attacks. This has paved way for new frauds, to be precise, old frauds done in slightly new manner.

2.1.4.1 Phishing as a trick of identity fraud

A successful phishing attack has a ripple impact which entraps multiple recipients. Individuals providing personal informations, join the thousands of victims who are fallen victimized to identity frauds. The aftermaths of successful phishing includes:
• The stolen credentials are utilised to make Illegal Purchases.
• New accounts are open by Identity frauds in the name of the victim, of which they might not be aware of.
• Victims of identity theft could spend several months, or even years, and vast amounts of money in recovering their good names and credit records, after they were damaged by identity thieves. They may be refused loans, education, housing and cars, due to bad credit reports. Victims usually experience a number of negative emotions, ranging from humiliation to anger and frustration (Federal Trade Commission, 2015).
• Phishing can cause consumers to lose confidence in the e-commerce industry. Phishing attacks are the basic element of trust essential for ongoing e-commerce. Consumers perceive the online environment as 'exceedingly risky' and that this perception 'could curb online spending' (Radcliff, 2015).

2.2 Social Engineering

2.2.1 What is Social Engineering?

Social engineering can be defined as fraudster tricking legit person to aid unlawful activities such as revealing PII or gaining in compatible entry.

The term “social engineering” is used, in regards with information security, to explain a criminal’s manipulation of a person in order to obtain credentials that would permit unauthorized entry to a computer system. Intruders or hackers try attempts to attain illicit entry to computer systems through many different types of attack. However, “social engineering” has a broader meaning which describes any circumstance in which a criminal uses social skills to deceive victim to reveal credentials.

2.2.2 Social and Technical Aspects of Phishing

Phishing is a criminal mechanism employing both Social engineering and Technical subterfuge to steal consumers’ personal identity data and financial account credentials. Social engineering tactics use fake emails to lure recipients to a fraudulent website that tricks the user to give away his personal information such as credit card number or username and password. In the social class of Phishing, the attackers employ subdomains and cousin domains to deceive users, better spelling and improved
psychological design of the request sent by means of email or website. Technical subterfuge tactics plant malicious software on user’s computer to directly steal their credentials, often by logging user’s keyboard strokes or loggers, seamlessly redirecting users to fraudulent websites by using proxies, use of DNS modifications to avoid takedown.

2.2.3 The emotional side of online social engineering

2.2.3.1 Psychological impact of Phishing on people

Executives who receive targeted phishing messages are losing confidence in email. Consumers, who, fear falling victim to a phishing attack, will not use online financial products, won’t open emails from their financial provider or enrol in online banking or bill payment (Forrester, 2014).

The Cybercriminals does not need technical skills; they depend on the integral weakness of mankind.

The most means of attacks which depend on social engineering tricks – and the very “human” responses raised are examined:

Fear or anxiety

The cyber criminals attempt to create them in the mind of a person to reveal their personal credentials. The most common tactics used is to impose misleading in user’s account. Failure to confirm a/c information will result in its closure. As a result the person is obliged to click upon the link contained in the mail. When the recipient clicks the link, he will be redirected to forged site requesting him to key in his credentials, to rectify the bogus trouble created. The stolen credentials are later utilised by the fraudster.

Trust

The criminals orient messages as if from social networking site itself, created so that victims are made to reveal their login credentials or download a Trojan.
Phishing attacks can be honed by means of publicly available personal information from social networks. The idea of using people’s social contacts to increase the power of an attack is analogous to the way in which the ILOVEYOU virus (Vbs.loveletter and variants), used email address books to propagate itself. Very easily and very effectively, a phisher can exploit social network data found on the Internet to increase the yield of a phishing attack. Internet users may be over four times as likely to become victims if they are solicited by someone appearing to be a known acquaintance (Jakobsson et.al, 2006).

Phisher look into Facebook or LinkedIn, for data mining details about association of individuals. Social networking sites are considered, when a spear phishing email is to be sent to a many number of commanders in an army base. Figure - 2.1 is the screenshot of message requesting the recipients’ to confirm their presence for a General’s retirement party. Upon clicking the link, Trojan will be downloaded to compromised system.

**Figure - 2.1: Spear Phishing Email Created to Misuse Trust**

General Clark is retiring next week, click here to say whether you can attend his retirement party

Spear phishing frauds have its impact on corporate sectors also. The victim employee will be sent an email as if from HR that projects to contain employee salaries in a PDF file, asking him to open or forward. The PDF attachment, will the clever cloak of a Trojan horse.

**Figure – 2.2: Fake Email Created to Misuse Trust in Workplace**
**Human Interest**

It evokes an emotional reaction because of people relation to it. They are a part of the news, and drive desire for more details. The cyber criminals use human interest stories to lure individuals. Figure – 2.3 is the bogus story of Michael Jackson’s death which projects to allegedly contain hidden truths for its viewers. The link will contain an executable extension, upon clicking will load Trojan.

**Figure – 2.3: Spam Email Created to Dupe Recipients**

**Human Interest Story**

Cyber fraudsters dupe users with up to date-event stories on forged webpages which look alike legit websites. In Figure – 2.4, a cyber-criminal has created replica of the CNN website that contains a link to a video on Turkey riots. The receivers of this mail will be lead to forged site which contains link and upon clicking to watch the video; the users would have downloaded malicious software into compromised systems.

**Figure – 2.4: Fake Download Message Created to Dupe Recipient**
Reward

The tax reporting frauds attackers design a message which states that, Tax reporting is a Citizens responsibility. The promise of a tax refund is a pecuniary reward, and the urgency in the mail will invoke victims. These frauds continue to be in the phishing portals in most nations, targeting taxpayers across the globe.

Another spam fraud associated with reward is developed to recruit money mules. In Figure – 2.5, the attackers look to cash out money stolen from individual’s bank or credit account in particular nations which target their citizens with fake job offers often titled “Money transfer agent” and “Transfer Manager.”

Figure - 2.5: Screenshot of Spam Email Created for Mule Recruitment

2.2.4 Methods of Attack using Social Engineering or Constituent of Social Engineering

Social engineering can be categorized as, man based and system based attacks. Computer or system based social engineering depends on technical deceits to deceive the victims to divulge credentials, allowing the attackers to gain entry into the system.

A pop-up window can be utilised, to trick the user that he has lost his network connectivity and to reconnect he need to re-enter his credentials. The credentials will
be messaged to a remote server through software that has been already installed in the compromised system.

The simplest and most efficient means of social engineering is still human based. It relies on interpersonal relations and deception, using the tools of trade such as flattery, intimidation, name-dropping, asserting authority and belittling. Any medium that provides one- to-one communications between people can be exploited, including face-to-face, telephone and electronic mail. All it takes is to be a good liar (Denning, 1999).

A good social engineer will do a bit of background research on the target company to get an idea of the basic structure and even some names. He can get access to the building roster. The roster quite often has a wealth of information such as the department names and sometimes even the names of the department heads. Another classic means of collecting information is dumpster diving, this refers to the analysis of the contents from a target’s trash bins (Heuer, 2003).

2.2.5 Classification of Computer security attacks

Computer security attacks can be categorised as three types namely, physical, syntactic, or semantic.

Physical attacks aim for the networking and physical infrastructure, whereas syntactic attacks target software and the semantic attacks, targets human.

Semantic attacks take advantage of individuals’ interaction with computers and the way they interpret messages, instead taking advantage of system flaws. Phishing attacks are instances of semantic attacks. Much less research has been done to try to investigate and address the human behaviour of semantic attacks.

2.2.5.1 Phishing is a kind of semantic attack

Phishing is a type of semantic attack that con people into divulging sensitive information in which victims are sent emails that deceive them into providing account numbers, passwords, or other personal information to an attacker. The phishers use techniques to make the user believe that information is being requested by a legitimate source. The attackers attempt to exploit the naïveté of some Internet users rather than
exploiting bugs in computer software. Phishing attacks get more sophisticated over time as attackers learn what techniques are most effective and alter their strategies accordingly. Those working to stop phishing have less information than the attackers about how users respond to various types of attacks. However, knowledge of users’ behavioural response is useful for developing techniques to educate users about phishing, for developing toolbars and other software designed to provide phishing-related warning indicators that users will actually pay attention to, and perhaps even for developing automated detection systems (Cranor, 2008).

In order to design counter measures that will be effective in mitigating these schemes, it is important to study the reasons behind people falling prey to fraudsters.

2.3 Cyber Crimes

2.3.1 Cyber Space and cyber crime

“The expression crime is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The offence is defined to mean as an act or omission made punishable by any law for the time being in force. Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity” (Code of Criminal Procedure, 2012).

Cybercrime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Cybercrimes have been reported across the world. Cybercrime is now amongst the most important revenue sectors for global organized crime. Because of this, the potential risks associated with malware have risen dramatically. Unlike in traditional crimes, the Information Technology infrastructure is not only used to commit the crime but very often is itself the target of the crime. Pornography, threatening email, assuming someone's identity, sexual harassment, defamation, Spam and Phishing are some examples where computers are used to
commit crime, whereas viruses, worms and industrial espionage, software piracy and hacking are examples where computers become target of crime.

2.3.2 Indian Cyber Crime Scenario

According to TRAI, currently, the country has 2.30 Crore internet subscribers. Increased penetration of IT services in BFSI and in the operations of SMBs, competition in the telecommunication sector, increase in government spending in IT infrastructure in PSUs and the exposure of Indian IT infrastructure to intruders are few of the factors which aid in the growth of Indian IT security market.

80% of Indian business enterprises have reported data theft through online hacking. The survey also indicates that as high as 90 percent of Indian companies have placed IT security as their priority investment domain and that the cost of computer crimes has reached a whopping USD 10 billion - India is ranked fifth in terms of E-Commerce security breaches (Frost & Sullivan, 2015).

Information security is a major cause of interest for Indian companies, with the threat of their network being hacked constantly increasing. SMBs need to develop proper IT infrastructure and Indian companies need to realize the potential threat of data theft. For this they will have to raise their level of investment in effective IT security systems. Cybercrimes on the rise, assess key emerging cybercrime trends related to organisations in India. It provides analysis on trends such as hacking and website defacement, corporate espionage, phishing and skimming (PwC, 2015).

The major cybercrimes reported, in India, are phishing, denial of services, defacement of websites, spam, computer virus and worms, pornography, cybersquatting, and cyber stalking.

Given the fact that nearly $120 million worth of mobiles are being lost or stolen in the country every year, the users have to protect information, contact details and telephone numbers as these could be misused. Nearly 69 per cent of information theft is carried out by current and ex-employees and 31 per cent by hackers.

The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India’s home PC owners are the most targeted sector
of its 37.7 million Internet users: Over 86 per cent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability (Symantec, 2014).

Cybercrime has been increasing at an alarming rate in India. The number of cybercrime cases registered under the IT Act in 2011 were 1791, an 85% increase since 2010 (966 in 2010). With an increase in cyber-crime organisations can build their competitive advantage by taking a strategic view of threat management that builds operational resilience and enables sustainable growth. While the threat of crisis is embedded in doing business today, it is worth noting that opportunity does not exist without threat. (National Crime Record Bureau, 2011).

The cybercrime cases registered number in 2014 was 2636, a 173% increase since 2010. A typical perpetrator of economic crime in India was male (almost 100 per cent), a graduate or undergraduate and 31-50 years of age. Further, over one-third of the frauds in the country were perpetrated by insiders and over 37 per cent of them were in senior managerial positions (PwC, 2015).

Indian constitution has a separate act to look after the Information Technology issues passed in the year 2000 as Information Technology Act, 2000 and later amended as ITAA 2008.

2.3.3 IT security Threats in India

83% of India companies are plagued by internal security breaches relating to loss of data or confidential information. The report highlights that 43 percent of such data loss is due to internal security breaches by employees. Further, as high as 28 percent of data theft is attributable to former employees who tend to share data of the previous organization with their current employer. The report also reveals that 42 percent of Indian enterprises suffer from financial losses due to internal security breaches and 35 percent have to deal with problems of intellectual property rights (Frost & Sullivan, 2015).
Figure – 2.6: Major Forms of Cyber Intrusions in India

Source: PwC, *IT security Threats in India, 2013*

The cybercrime cost borne by Indian companies annually, amounts to INR 341 billion. The research report also states that Indians aged between 18 and 31 years of age, who primarily use internet, are more prone to suffer from cybercrimes. Nearly 70 percent of adult users of internet have online adults have suffered from cybercrimes. Every second around 16 adults fall victim to cybercrime, translating into over a million victims of cybercrimes in India every day. The major form of cyber-attack is considered to be internet phishing, which constitutes 50 percent of all cyber-attacks in computers and smart phone devices (PwC, 2015).