CYBER LAWS AND CRIMES IN INDIAN BANKING SECTOR

Madhulika V. Bhat
Lecturer
Poornaprajna College, Udupi
madhulika.pb@gmail.com

ABSTRACT

In today's world we completely relay upon technology and electronics to keep everything running smoothly. No matter where we go, there is some sort of Technology that has a drastic influence on life. Whether it to be the grocery store, shopping, service stations, movie theatres most of these places would cease to be able to operate if there were no more access to the technology they have become dependent. At the same time that the world has become overly dependent in technology, criminals have taken advantage of this situation to use it for their benefit and to make committing crimes easier for them and in many cases people are victims can unknowingly make themselves as targets simply by not protecting their presence in this technical world. As technology evolves and people undoubtedly become increasingly more, dependent on this technology they will get more and more careless with the important information. As technology grows and cybercrime because more prevalent then so do the steps and precautions taken to prevent it. The study focuses on cybercrimes and awareness of laws with regard to udupi district.

KEYWORDS: Cyber bullying, Cyber laws, Banks, Protection

Introduction

When Internet was developed, the establishing fathers of Internet hardly had any preference that Internet could transform itself into a impressive revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the unstipulated nature of the Internet, it is possible to engage into a variety of criminal activities with liberty and people with intelligence, have been utterly misusing this aspect of the Internet to extend criminal activities in cyberspace. Hence the need for

Cyber laws in India.

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber law is a very technical field and that it does not have any air to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives. Cyber law does concern you. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal outlook. From the time you register your Area Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails, to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyber law issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tense up your belts and take note of Cyber law for your own benefit.

Literature Review:

- This chapter is a review of the current literature on recent efforts to research cyber bullying and offensive discourse among adolescents in cyberspace
- In Shaheen Shariff (2009), Confronting Cyber bullying: What Schools Need to Know to Control Misconduct and Avoid Legal Consequences book
- Indian IT act 2000 article in magazines
- Section 66A in the amended IT Act deals with these crimes. Sending any message (through a computer or a communication device) that is grossly offensive or has menacing character; any communication which he/she knows to be false, but for the purpose of causing insult, annoyance and criminal intimidation comes under this section. This crime, under the current IT/Cyber/Criminal laws in India is punishable up to three years with a fine.

Objective

- To know the awareness and incidents relating to about cyber crimes

- To understand the types of cybercrimes concerning the banking and financial sector and their related impacts

Cyber Crime In Banking Sector

Cyber Crime can be simply stated as crimes that involve the use of computer and a network as a medium, source, instrument, target, or place of a crime. With the growing aspect of e-commerce and e-transactions, the economic crime has floated towards the digital world. Cybercrimes are increasing globally and India too has been witnessing a sharp increase in cybercrimes related cases in the recent years. In 2016, a study by Juniper Research estimated that the global costs of cybercrime could be as high as 2.1 trillion by 2019. However such estimates are only indicative and the actual cost of cybercrime including unreported damages is beyond estimation. Cyber Crimes can be broadly classified into categories such as cyber terrorism, Cyber-bullying, Computer Vandalism, Software Piracy, Identity Theft, Online Thefts and Frauds, Email Spam and Phishing and many more. However, from the aspect of financial cybercrimes committed electronically, the following categories are predominant:

- Hacking: It is a technique to gain illegal access to a computer or network in order to steal, corrupt, or illegitimately view data
- Phishing: It is a technique to obtain confidential information such as usernames, passwords, and debit/credit card details, by impersonating as a trustworthy entity in an electronic communication and replay the same details for malicious reasons
- Fishing: It is the criminal practice of using social engineering over the telephone system to gain access to private personal and financial information from the public for the purpose of financial reward
- E-mail Spoofing: It is a technique of hiding an e-mail’s actual origin by forged the e-mail header to appear to originate from one legitimate source instead of the actual originating source
- Spamming: Unwanted and unsolicited e-mails usually sent in bulk in an attempt to force the message on people who would not otherwise choose to receive it are referred to as Spam E-mails
- Denial of Service: This attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service by "flooding" a network to disallow legitimate network traffic, disrupt connections between two machines to prohibit access to a service or prevent a particular individual from accessing a service
- Advanced Persistent Threat: It is characterised as a set of complex, hidden and on-going computer hacking processes, often targeting a specific entity to break into a network by avoiding detection to gather sensitive information over a significant period of time. The attacker usually uses some type of social engineering, to gain access to the targeted network through legitimate means
- Advanced Persistent Threat: It is characterised as a set of complex, hidden and on-going computer hacking processes, often targeting a specific entity to break into a network by avoiding detection to gather sensitive information over a significant period of time. The attacker usually uses some type of social engineering, to gain access to the targeted network through legitimate means. Successful advanced persistent threat campaigns can result in costly data breaches
- ATM Skimming and Point of Sale Crimes: It is a technique of compromising the ATM machine or POS systems by installing a skimming device atop the machine keypad to appear as a genuine keypad or a device made to be affixed to the card reader to look like a part of the machine. Additionally, malware that steals credit card data directly can also be installed on these devices. Successful implementation of skimmers cause in ATM machine to collect card numbers and personal identification number (PIN) codes that are later replicated to carry out fraudulent transactions

Overview Of Internet Banking In India

The Indian baking industry is enjoying a jubilant growth. With the credit card and debit card users increasing every day and new technologies like internet wallets slowly gaining popularity, the financial transactions are touching all-time highs. This firm advancement in the intensifying paper less transactions numbers where a total of 9545797438 transactions were commenced using credit and debit cards in the year 2015 alone .In order to provide improved support for cashless transactions, a sensible increase in the number ATM and POS machines is inevitable across India in 2015. The cases related to cybercrimes have grown ruthlessly due to the increase in mobile devices with internet connectivity. Smartphones are nowadays used for numerous online activities like internet banking, online shopping, paying utility bills and are constantly in the eyes of the criminals to obtain access to confidential information. Amongst the various motivations for committing a cybercrime, Financial Gain remains the constant winner for the past many years overtaking other motives including revenge, extortion and political causes. Alarmingly, simple phishing attacks enjoy a success rate of 45% due to lack of awareness regarding the common safeguards to protect against the shrewd cyber criminals. The span of cybercrime can be estimated from the figures of 3855 cybercrimes committed for financial gain. (NTRO) and 534 phishing incidents (CERT-In) in year 2015. These incidents on the span of cybercrime can be estimated from the figures of 3855 cybercrimes committed for financial gain (NTRO) and 534 phishing incidents (CERT-In) in year

2015. These incidents only correspond to the reported incidents and do not comprise the incidents that went unreported and/or unnoticed. Banks across the globe are increasing becoming prime targets of distributed denial-of-service (DDoS) attacks launched sometimes as a part of the plan to distract the security professional's attention to the exhausting resources, while carrying out some additional dangerous activity in parallel like insertion of malware, or tampering with the 'safeguarding the internet banking sector' Financial organizations in today's date require well positioned cyber security teams with distinguished digital leaders. According to PWC‟s year's global economic crime survey, 2016, too many organisations are leaving first response to their IT teams without adequate intervention or support from senior management and other key players.

Legal Issues

Incidents like these are growing sharply with poor knowledge among users about how to protect accounts. Sharing one's passwords with others too is proving dangerous. Prof. Madabhushi Sridhar, a cyber-laws expert at NALSAR University, says the crimes cited above come under the bracket of invasion of privacy. He says Section 66A in the amended IT Act deals with these crimes. Sending any message (through a computer or a communication device) that is grossly offensive or has menacing character; any communication which he knows to be false, but for the purpose of causing insult, annoyance, criminal intimidation comes under this section. This crime, he says, is punishable up to three years with a fine. Prof. Sridhar, who has just completed a book on cyber laws, feels that punishments under the IT Act are insufficient. "They should be read with the Indian Penal Code. This will be an effective method to check cybercrimes," he says. Prof. Sridhar also represents the Institute of Global Internet Governance and Advocacy (GIGA) at the Law University. GIGA conducts research on the Internet and takes up advocacy and training programmes on Internet Governance. "We already have anti-voyeurism provisions in the IT Act under Sec. 66E," Mr Sunil Abraham, Executive Director of Centre for Internet and Security, says.

This offence is punishable with 'imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.' Repeated harassment aka cyber bullying can be addressed using the already over-broad provisions under Sec. 66A. Unfortunately this Section goes too far and can be used to censor legitimate speech.

"Security and privacy awareness in India is very poor. It would be very useful if both the government and civil society was more aggressive in awareness raising and triggering change in behaviour. Unfortunately this is a bit like smoking - even though people are aware of the issues - they engage in risky behaviour online," he says.

Lack of Data

Pavan Duggal, Chairman of Cyber Law Committee and Cyber laws expert said there is no specific data on cybercrime in India and the data available with the NCRB (National Crimes Records Bureau) of around 900 cases for overall cybercrime is also doubtful. "The solution is to make cyber laws more strict as current law under IT Act 2000 is a bailable offence with three years' imprisonment and a fine," he points out. "IT Act 2000 has to be re-amended to specific provisions pertaining to cyber bullying. Further, cyber bullying needs to be made a serious offence with minimum five years imprisonment and a fine of Rs. 10 lakh. Unless you have deterrence in law it will be a continuing offence," he observes. Fortunately, there are some safeguards which can help prevent such acts of cyber offences. In most cases, the acts of bullying or blackmailing are done by someone close to the victims. People should make it a point to keep their Internet identities very safe. One should not disclose their identities such as passwords or hint questions to anyone – no matter how close they are. Parents should keep an eye on their children who are addicted to the Internet. They should inform and educate their children on the clear and present dangers that lurk on the Net. They should also teach the importance of respecting others' privacy apart from taking precautions to keep their private space very safe.

Methodology

The analysis is based on primary data and secondary data. **Primary data** was collected from 50 retired employees (age group between 60 to 65) of different fields, who have smart phones and uses internet and mobile banking facilities. **Secondary data** was collected from various journals, IT act 2000, Govt reports and survey etc.

Hypothesis

H0: There is no association between age and cyber laws
H1: Significant association between awareness about cyber laws
H2: Significant result with concern to cybercrimes and types
H3: Out of 50 samples (randomly selected) 20 women 30 men

Findings

- Most of the employees don't use smart phones to make use of internet banking facilities
- Not taking necessary actions even though they get the spam messages.
- Limited knowledge about the cyber laws

- Avoidance of cyber crimes

Recommendations

- Section 66A in the amended IT Act deals with these crimes. Sending any message (through a computer or a communication device) that is grossly offensive or has menacing character; any communication which he/she knows to be false, but for the purpose of causing insult, annoyance and criminal intimidation comes under this section. This crime, under the current IT/Cyber/Criminal laws in India is punishable up to three years with a fine
- “We have helped many people take legal action against cyber bullying, including removal of fake profiles, deletion of derogatory content and responding to email abuse. Most people decide to take legal action if these online threats start affecting their real lives, and hinder their social image and peace of mind,” says Rohan Mahajan, Founder of LawRato.com
- Security and privacy awareness in India is very poor. It would be very useful if both, the government and civil society were more aggressive in raising awareness and triggering change in behaviour
- Unfortunately, this is a bit like smoking – even though people are aware of the issues, they engage in risky behaviour online. The solution is to make cyber laws stricter as current law under the IT Act 2000 is a bailable offence with three years’ imprisonment and a fine
- The IT Act 2000 should to be re-amended to specific provisions pertaining to cyber bullying. Further, cyber bullying needs to be made a serious offence with minimum five years imprisonment and a fine of Rs. 10 lakh. Unless you have deterrence in law, it will continue to be a prevalent offence

Conclusion

It can be seen that the threat of computer crime is not as big as the authority claim. This means that the methods that they introducing to battle it represents an unwarranted attack on human rights and is not proportionate to the threat posed by cyber-criminals. Part of the problem is that there are no reliable statistics on the problem; this means that it is hard to justify the increased powers that the Regulation of Investigatory Powers Act has given to the authorities. These powers will also be ineffective in dealing with the problem of computer. The international contracts being drawn up to deal with it are so unclear that they are bound to be ineffective in dealing with the problem. It will also mean the civil liberties will be unfairly affected by the terms of the agreements since they could, possibly, imply that everybody who owns a computer fitted with a modem could be suspected of being a hacker. The attempts to outlaw the possession of hacking software could harm people who trying to make the internet more secure as they will not be able to test their systems; therefore the legislation could do more harm than good.

References

- Dr. Tewari R.K., Sastry P.K. & Ravikumar K.V., 'Computer Crime and Computer Forensics.' Jain Book Agency, Delhi, 2002
- Dr Gandhi; K.P.C, 'Introduction to computer related crimes.' CBI Bulletin, Delhi
- Arun Kumar Gupta, 'Cyber Crime and Jurisdictional problem.' CBI Bulletin. June-December 2006.(article)
- Susan W. Brenner, 'At light speed: Attribution & Response to Cyber crime/Ten'orism/Warfare.' The Journal of Criminal Law & Criminology. Vol. 97, No. 2, winter 2007.