Cyber Fraud in Social Media World: A Legal Perspective

• **AISHWARYA DASH**
PRACTICING INDIAN ADVOCATE

Introduction- The Concept of Cyber Fraud

In the era of cyber world as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term 'Cyber' became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. Due to increase in the number of citizens, misuse of technology in the cyberspace was clutching up which gave birth to cyber-crimes at the domestic and international level as well. It is really hard to define such a broad term as cyber fraud. There is, however, a few general characteristics you find in all cyber scams. Most of the scams are done by e-mail (Spam). They entice users to give them critical information like usernames, passwords, credit card information, or other types of account information. Most of these e-mails can easily be identified as fraudulent, by identifying a couple of general characteristics.[1] Broadly speaking, cyber fraud means the use of internet to get money, goods, etc., from people illegally by deceiving them.

Definition

The word Crime carries its general meaning as "a legal wrong that can be followed by criminal proceedings which may result into punishment" whereas Cyber Crime may be "unlawful acts wherein the computer is either a tool or target or both". Cyber-crimes include hackers vandalizing your site, viewing confidential information, stealing trade secrets or intellectual property with the use of internet. Cyber-crimes also includes criminal activities done with the use of computers which further perpetuates crimes i.e. financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail, spoofing, forgery, cyber defamation, cyber stalking, unauthorized access to Computer system, theft of information contained in the electronic form, e-mail bombing, physically damaging the computer system etc.[2] The word internet fraud and cyber fraud are used interchangeably. Internet has spawned novel and interesting methods to defraud individuals and companies. Internet fraud is a form of white-collar crime whose growth may be as rapid and diverse as the growth of Internet itself. The term internet fraud may be broadly defined as any fraud committed through or with the aid of computer programming or internet related communications as websites, emails and chat rooms.[3]

Cyber Frauds & Types

Rising at alarming rate, the number of cyber-crimes in India may touch a humungous figure of 3,00,000 in 2015, almost double the level of last year causing havoc in the financial space, security establishment and social fabric, an ASSOCHAM-Mahindra SSG study warned. While releasing the joint study on "Cyber and Network Security Framework" Mr. D.S Rawat, Secretary General ASSOCHAM said, "What is causing even more concern is that the origin of these crimes is widely based abroad in countries including China, Pakistan, Bangladesh and Algeria among others". As per the study findings, during 2011, 2012, 2013 and 2014 years, a total number of cyber-crimes registered were 13,301, 22,060, 71,780 and 62,189 (till May). Currently, the cyber-crimes in India is nearly around 1,49,254 and may likely to cross the 3,00,000 by 2015 growing at compounded annual growth rate (CAGR) of about 107 per cent. As per the findings, every month nearly 12,456 cases registered in India. Phishing attacks of online banking accounts or cloning of ATM/Debit cards are common occurrences. The increasing use of mobile/smart phones/tablets for online banking/financial transactions has also increased the vulnerabilities to a great extent. The maximum offenders came from the 18-30 age group, adds the report.[4]

Online Investment Newsletters:

Hundreds of online investment newsletters have appeared on the Internet in recent years. Many offer investors seemingly unbiased information free of charge about featured companies or recommending "stock picks of the month". While legitimate online newsletters can help investors gather valuable information, some newsletters are tools for fraud.[5]

Bulletin Boards:

Online bulletin board-whether newsgroups, Usenet, or web-based-have become an increasingly popular forum for investors to share information. Bulletin boards

[1] Cyber Top Cops, Cyber Fraud, Scam, Hoaxes-Definition and Prevention, http://www.cybertopcops.com/anti-fraud.php (Last visited on: 14.6.2018).
[2] Dhawesh Pahuja, Cyber-crimes and the Law, 17th July 2011, http://www.legalindia.com/cyber-crimes-and-the-law/ (Last Visited on: 14.6.2018).
[3] Nandan Kamath, Law Relating to Computers Internet and E-Commerce, 5th ed., 2015, 219.
[4] ASSOCHAM India, Cyber-crimes in India is likely to cross 3,00,000 by 2015: Study, 4th January, 2015, http://www.assocham.org/newsdetail.php?id=4821 (Last visited on: 14.6.2018).
[5] Nandan Kamath, Law Relating to Computers Internet and E-Commerce, 5th ed., 2015, 220.

typically feature "threads" made up of numerous messages on various investment opportunities.[6]

Email Online Spams:

Because "spam"- junk email- is so cheap and easy to create, fraudsters increasingly use it to find investors for bogus investment schemes or to spread false information about a company. Spam allows the unscrupulous to target many potential investors. Using a bulk email programme, spammers can send personalised messages to thousands and even millions of Internet users at a time.[7]

Click fraud:

The latest scam to hit the headlines is the multi-million dollar Click fraud which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via spyware, the affiliate is then paid a commission on the cost-per-click that was artificially generated. Affiliate programs such as Google's Adsense capability pay high commissions that drive the generation of bogus clicks. With paid clicks costing as much as US$100[verification needed] and an online advertising industry worth more than US$10 billion, this form of Internet fraud is on the increase.[8]

Nigerian Scam:

Nigerian or Frauds 409 or 419 are basically the lottery scam in which some overseas persons are involved to cheat innocent persons or organizations by promising to give a good amount of money at nominal fee charges. Their intention is to steal money in the form of fee against the lottery prize.[9]

Banking frauds:

Most of the online banking frauds are conducted either through phishing, stealing of banking information or through cloning of credit/debit cards. Banking frauds can be done in following way[10]:

- Stealing of the original credit/debit cards and using the cards at shopping merchants (POS purchases)
- Cloning/duplication of credit/debit card
- Phishing scams where the information has been revealed by the customer himself
- Leakage of PIN/credit card/debit card numbers by the handlers of such information/payment gateways/banks (voluntary or involuntary like hacking, physical intrusion, data breach).
- Usage of stolen/duplicate/cloned mobile SIM card to receive one-time password (OTP) of mobile/net banking and transaction made using such information.

Phishing: Most Popular Way of Committing Cyber Fraud

Definition of Phishing

Phishing means sending an e-mail that falsely claims to be a particular enterprise and asking for sensitive financial information. Phishing, thus, is an attempt to scam the user into surrendering private information that will then be used by the scammer for his own benefit. Phishing uses 'spoofed' e-mails and fraudulent Web sites that look very similar to the real ones thus fooling the recipients into giving out their personal data. Most phishing attacks ask for credit card numbers, account usernames and passwords. According to statistics phishers are able to convince up to five per cent of the recipients who respond to them.[11] Phishing is the method used to steal personal information through spamming or other deceptive means. There are a number of different phishing techniques used to obtain personal information from users.

Types of Phishing Attack

- Spear Phishing: "Spear phishing" is a colloquial term that can be used to describe any highly targeted phishing attack. Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.[12] Spear phishers send spurious e-mails that appear genuine to a specifically identified group of Internet users, such as certain users of a particular product or service, online account holders, employees or members of a particular company, government agency, organization, group, or social networking website. Because it comes from a known and trusted source, the request for valuable data such as user names or passwords may appear more plausible.
- Clone Phishing: Clone phishing is a type of phishing attack where hacker tries to clone a web site that is victim usually visits. The clone web site

[6] Ibid.
[7] Nandan Kamath, Law Relating to Computers Internet and E-Commerce, 5th ed., 2015, 220.
[8] Ibid.
[9] Internet banking frauds, http://www.worldjute.com/ebank1.html (last visited on: 14.6.2018).
[10] Amartya Bag, Online banking frauds in India: How to recover lost money using Information Technology Act, 2000?, 18th April 2015, http://blog.ipleaders.in/online-banking-frauds-in-india-how-to-recover-lost-money-under-information-technology-act-2000/#ixzz445pbJlY5 (Last visited on: 14.6.2018).
[11] ICICI Bank Phishing, http://indiaforensic.com/icicihack.htm (Last Visited on: 5.4.2016).
[12] Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, Binational Working Group on Cross-Border Mass Marketing Fraud October 2006, 8, https://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf (Last visited on: 14.6.2018).

usually asks for login credentials, mimicking the real websites. This will allow the attackers to save these credentials in a text file, database record on his own server, then the attacker redirects his victim to the real websites as a authenticated user.[13]

- Redirection and Other Malicious Code-Based Schemes: Another technique that phishers use is to cause targeted Internet users to unknowingly download certain forms of malicious computer code into their office or home computers. One type of phishing scheme that uses malicious code is the so-called "redirection" scheme. Ordinarily, when an Internet user types the address of a particular website (such as "http://reallymybank.com") into an Internet browser, the computer directs the user to the correct website.[14]
- Phone Phishing: This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service, is dialled, voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source.[15]
- Vishing: A phishing technique that has received substantial publicity of late is "vishing," or voice phishing. Vishing can work in two different ways. In one version of the scam, the consumer receives an e-mail designed in the same way as a phishing e-mail, usually indicating that there is a problem with the account. Instead of providing a fraudulent link to click on, the e-mail provides a customer service number that the client must call and is then prompted to "log in" using account numbers and passwords. The other version of the scam is to call consumers directly and tell them that they must call the fraudulent customer service number immediately in order to protect their account. Vishing criminals may also even establish a false sense of security in the consumer by "confirming" personal information that they have on file, such as a full name, address or credit card number.[16]

Regulation Under Indian Law

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on e-commerce in the year 1996. The General Assembly of United Nations passed a resolution in January 1997 *inter alia*, recommending all States in the UN to give favourable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record.

It is against this background the Government of India enacted its Information Technology Act 2000 with the objectives, which is reproduced as under for ready reference:

"*An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.*"

The Information Technology Act, 2000, was thus passed as the Act No.21 of 2000, and got Presidential assent on 9th June, 2000 and was made effective from 17 October 2000. The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber-crimes.

The Information Technology Act was amended in the year 2008 which got the President assent on 5 Feb 2009 and was made effective from 27 October 2009. Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in

[13] Dr. M. Nazreen Banu, A Comprehensive Study of Phishing Attacks, International Journal of Computer Science and Information Technologies, Vol. 4 (6) , 2013, 783-786, 1, http://www.ijcsit.com/docs/Volume%204/Vol4Issue6/ijcsit2013040607.pdf (Last Visited on: 14.6.2018).

[14] Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, Binational Working Group on Cross-Border Mass Marketing Fraud October 2006, 9, https://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf (Last visited on: 14.6.2018).

[15] Junxiao Shi, Sara Saleem, Phishing, 2, https://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic5-final/report.pdf (Last visited on: 5.4.2016).

[16] Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, Binational Working Group on Cross-Border Mass Marketing Fraud October 2006, 10, https://www.justice.gov/sites/default/files/opa/legacy/2006/11/21/report_on_phishing.pdf (Last visited on: 14.6.2018).

technology based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA.[17] The Act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person. There are some specific exclusions to the Act (i.e. where it is not applicable) as detailed in the First Schedule, stated below[18]:

- negotiable instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
- a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
- a trust as defined in section 3 of the Indian Trusts Act, 1882
- a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition
- any contract for the sale or conveyance of immovable property or any interest in such property;
- any such class of documents or transactions as may be notified by the Central Government.

Jurisdictional Issue

The eminent question of discussion is that if a crime is committed on a computer or computer network in India by a person resident outside India, then can the offence be tried by the Courts in India? According to Section 1(2) of Information Technology Act, 2000, the Act extends to the whole of India and also applies to any offence or contravention committed outside India by any person. Further as per Section 75 of the I.T. Act, 2000 which also mentions about the applicability of the Act for any offence or contravention committed outside India. According to this section, the Act will apply to an offence contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India. A Police officer not below the rank of Deputy Superintendent of Police should only investigate any offence under this Act. (Sec. 78 of I.T Act, 2000).[19] But the problem still prevails because without a duly signed extradition treaty or a multilateral cooperation arrangement, trial of such offences and conviction is a difficult proposition as the physical presence of the offender still remains outside the jurisdiction of the courts of India.

The Laws on Phishing fraud in India

The phishing fraud is an essentially it is a cyber-crime and it attracts many penal provisions of the Information Technology Act, 2000 as amended in 2008 adding some new provisions to deal with the phishing activity. The following Sections of the Information Technology Act, 2000 are applicable to the Phishing Activity:

- Section 66: The account of the victim is compromised by the phisher which is not possible unless & until the fraudster fraudulently effects some changes by way ofdeletion or alteration of information/ data electronically in the account of the victim residing in the bank server. Thus, this act is squarely covered and punishable u/s 66 IT Act.
- Section 66A: The disguised email containing the fake link of the bank or organization is used to deceive or to mislead the recipient about the origin of such email and thus, it clearly attracts the provisions of Section 66A IT Act, 2000
- Section 66C: In the phishing email, the fraudster disguises himself as the real banker and uses the unique identifying feature of the bank or organization say Logo, trademark etc. and thus, clearly attracts the provision of Section 66C IT Act, 2000.
- Section 66D: The fraudsters through the use of the phishing email containing the link to the fake website of the bank or organizations personates the Bank or financial institutions to cheat upon the innocent persons, thus the offence under Section 66D too is attracted.

The Information Technology Act, 2000 makes penal provisions under the Chapter XI of the Act and further, Section 81 of the IT Act, 2000 contains a non obstante clause, i.e. the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. The said non-obstante clause gives an overriding effect to the provisions of the Information Technology Act over other Acts prevalent in India and which also including the Indian Penal Code.[20] The aforesaid penal provisions of the IT Act, 2000 which is attracted to the phishing scam are however been made bailable by virtue of Section 77B IT Act intentionally in view of the fact that there is always an identity conflict as to the correct or accurate identity of the person behind the alleged phishing scam and there is always a smokescreen behind the alleged crime as to the identity of the person who has actually via these online computer resources have or have not committed the offence and in view of the possible misuse of the penal

[17] Cyber Laws in India, http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf (Last Seen on 20.06.2018)

[18] First Schedule of Information Technology Act, 2000, http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf (Last Seen on 20.06.2018)

[19] Ajay Thakur, All you need to know about Cyber Laws in India, 03.03.2017, https://blog.ipleaders.in/need-know-cyber-laws-india/ (Last seen on 20.06.2018).

[20] Spandan Pujari, Prevention and Regulation of Phishing in Cyber World: National and International Framework, https://www.academia.edu/8702857/Cyber_Law_-_Prevention_and_Regulation_of_Phishing_in_Cyber-Space_National_and_International_Framework (Last Visited on: 14.6.2018).

provision for cyber offences are contained in the IT Act, the offence is made bailable.

Conclusion

Phishing attacks are still successful because of many inexperienced and unsophisticated internet users. The last years have brought a dramatic increase in the number and sophistication of such attacks. This paper provides a broad survey of various phishing types which are used by attackers to steal the sensitive information. This study clearly shows that phishing techniques enables the attackers to steal the information efficiently. Our future work is to compare various types of anti-phishing techniques and choose the best one for further research. Users have become more aware of phishing crimes and how to identify unsophisticated phishing sites. In response, criminals are using web browser vulnerabilities and obfuscation techniques to create phishing scam pages that are more difficult to differentiate from legitimate sites; thus users can become victims even if they are aware of phishing scams. Phishing is a form of criminal conduct that poses increasing threats to consumers, financial institutions, and commercial enterprises in Canada, the United States, and other countries. Because phishing shows no sign of abating, and indeed is likely to continue in newer and more sophisticated forms, law enforcement, other government agencies, and the private sector in both countries will need to cooperate more closely than ever in their efforts to combat phishing, through improved public education, prevention, authentication, and binational and national enforcement efforts. Phishing is a major concern in the contemporary e-commerce environment in India and will continue to be so because of the lack of awareness among the Internet users who are new to the internet realm. There is no silver bullet to thwart the phishing attack. However, it has been noticed in the most of the phishing scams worldwide particularly in India that the hacker succeeds in phishing attempt due to the uninformed, gullible customers who without knowing that they are being trapped unwittingly pass on the information asked for by the fraudster. Therefore, the awareness and customer education is the key here to fight the menace of the "Phishing" apart from mitigating or preventative measures. The law enforcement agencies, the legislature, the industry should come together and coordinate in their fight against the menace of the Phishing.

