World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2015; 1(1): 21-23
www.wwjmrd.com
e-ISSN: 2454-6615

Kumar Harsh
Final Year, B.Tech (E.T.C.), M.B.A., Business Analyst, Capital Via Global Research, Indore, M.P, India

Tanya Singh
4th Year, BBA, LLB (Hons.), Amity Law School, Noida, UP, India

Pramod Kumar Singh
Professor, Veer Kunwar Singh University, Ara, Bihar, India

Correspondence:
Kumar Harsh
Final Year, B.Tech (E.T.C.), M.B.A., Business Analyst, Capital Via Global Research, Indore, M.P, India

Emerging threats of cyber crimes

Kumar Harsh, Tanya Singh, Pramod Kumar Singh

Abstract
Information technology (IT) is now an integral part of day to day life. One cannot imagine socio-economic development without help of IT. Information technology is the fast growing technology in the world and it is now recognised as a measure of development. Due to widespread use of the technology by Government, Corporate and industrial sectors, the criminal abuse of the technology is also increasing day by day. Cyber crimes in India have soared nearly 350 percent within three years but the law relating to cyber offences remain to be inadequate. National Crimes Record Bureau (NCRB) statistics shows that the number of recorded cases of cyber crimes has jumped to 4356 from 966 in three years. The challenges for India are much greater because of vast population of about 302 million internet users. About 24% of population is expected to be online very soon. Those who are prosecuted and arrested for cyber crimes are mostly young people between ages of 18-20 years. Cyber attacks are becoming more and more sophisticated and brazen day by day. Security analysis called the year 2013 as mega breach year with about 62% increase in the breach as compared to 2012. Both sophistication and brazenness are apparent in recent attacks. The offences like spear fishing, intelligent emails etc. targets at individuals by making emotional connection. The experts say that there are now more apprehensions of attacks on sophisticated cars medical devices etc. Children are venerable to risky behaviours on virtual space. If any child remains hooked to the internet for long hours, there is high risk and preventive care must be taken for this because paedophiles, kidnappers, sex offenders and black mailers etc. are on the prowl on the virtual space. Everyone should take precautions while using bank's debit or credit cards as well as while online internet transactions.

Keywords: Cyber Crimes, Internet, Virtual Space

1. Introduction
Information technology is one of the fastest growing technologies in the world. Rapid transformations are taking place from a system of control due to liberalisation and globalization of information technology.[1] The information is being recognised as a source of development of countries. The timely availability of accurate, reliable and constant information on various accounts is an essential factor for the Government, Corporate and Industrial sectors. Whole world is repeatedly gearing up to meet the challenges of managing the changed environment. The usual forms of cyber crimes, such as hacking, cracking, e-mail spoofing, stalking, phreaking, carding etc. has gone ahead and several new forms of cyber crimes are coming into lime light.

Cyber crimes are India has soared nearly 350% within three years, but the law remains inadequate. National Crime Records Bureau (NCRB) statistics show that number of recorded cases of cyber crimes has jumped to 4356 from 966 in the three years upto 2013, and thus India being more susceptible to digital attacks because of the increasing number of net users in the fast-growing economy.[2] "*Illegal gains*" and "harassment" are the top cyber crimes motives, though the majority of the crimes were registered under the "*others*" category i.e. 2,144 cases in 2013. The analysis says that such a high number of cases being pigeon holed in this section imply that the current laws and regulations are not expansive and adequate enough to tackle the cyber crimes.

The challenges for India is much greater mainly because of its vast population of internet users i.e. 302 million by the end of 2014, and the population is set to overtake the United States this year which country is having the second larger number of netizens after China. About 24% of population is expected to be online and those who are prosecuted and arrested under the laws relating to cyber crimes are mostly young people. Data shows that such offenders are between ages of 18-30 and about 1,638 persons were arrested in 2013 for cyber offences.[3]

The rapid increase in cyber crime may also have been caused due to insufficiency in the legal system Activists say that some cyber laws are too draconian and affects the citizen's fundamental rights. For example, anyone found guilty under section 66 A of the Information Technology (IT) Act, 2000 (which deals with "*offensive*" massage sent through the computer or other personal communication devices) can be prosecuted and punished up to three years. Two girls of Maharashtra were arrested under this particular section in 2012 for their comments posted on face-book on the event of Mumbai being shut down for the funeral of *shiv-sena* founder Bal Thackeray. Various sections of the IT Act are often bitterly criticised for being blindly copied from British and American Laws, which may not be reasonable and proper for India's scenario. To prevent abuse, the Apex Court ruled in 2013 that arrest could only be made after clearance is obtained from an inspector by General of Police in the city and a Superintendent of Police in a district obtained. The provision of Sec. 66A of I.T. Act has now been ultimately been declared *null* and *void* by Apex Court in a recent pronouncement made in March, 2015 as the proviso affects the fundamental of rights of speech and expression of citizens.

Cyber attacks are becoming more and more sophisticated and brazen day by day. Global Security Analysts' called 2013, the year of the mega breach, with about 62% increase in the number of data breaches as compared to 2012.[4] There were 91% increase in targeted attack. Both sophistication and brazenness of cyber crimes were apparent in these recent attacks. '*Spear fishing'*, which involves 'intelligent emails', 'targeting at individual', 'catching target off shared by making emotional connection', enticing emails and with phone calls to win the victims trust, focusing in "watering holes" which are frequented by targets and throwing bails like free broad band connection etc. show the expanded arsenal of cyber crimes.

The experts say that there are now serious apprehensive of attacks on computer operated sophisticated and automatic cars and medical devices. '*Smart cars'* are at high risk of being hacked. The future smart cars may be safer, smarter and offer them grater high-tech gadgets but without improved security, such vehicles run at greater risk of being hacked. Government are also not prepared to combat the looming threat of "online murder" as cyber criminals may exploit internet technology to target victims the European policing agency has warned.[5] Interpol has also warned that there is expected rise in injury and possible deaths caused by computer attacks on critical safety equipments. Police Forensic Technology is needed to adopt and grow to meet the danger posed by the criminal abuse of internet.

Children are venerable to risky behaviour on virtual space. If any child remains hooked to the internet for long hours, there is high risk and therefore preventive measures must be taken for this. According to a survey conducted by online security firm MCAFEE, Parents in the city should take extra precautions because paedophiles, kidnappers, sex offenders and black mailers etc. are on the prowl on the virtual space. The teens in Kolkata are among the most venerable to risky behaviour on the internet. A survey of children aged 8-12 years across metros like Kolkata, Delhi, Mumbai, Chennai, Bangalore, Hyderabad and Ahmadabad has triggered alarm bells among parents as awareness about threats on social networking platforms is the lowest in the city. Despite the age eligibility for face-book being 13 years, three out of four (70%) children admitted to use face-book by dressing up their age.[6]

Finance sector is also under serious threats as cyber offenders are adopting new ways to steal bank's credit/ debit cards, pin numbers and other account's informations. Credit/ debit cards fraud cases in the city have seen a sharp rise of almost upto 400% from 32 cases lodged in 2013 to 159 cases in 2014. Cyber experts says that frauds are constantly adopting new methods, with the advent of new social networking and new technology, cyber offenders too have adopted innovative methods to steal information's from unsuspecting victims. *Accounts takeover friendly fraud*, *Cloning/ malware*, *skimming*, *phishing* etc. are the common finance related offences committed nowadays. Some case-studies may help us to understand the emerging new threats in the field of cyber crime:-

i. **Account takes over**- It is traditionally a most popular non technology method in which fraudsters manipulates consumers account.

On December 2014, a 52 years old man filed a complaint with the police after he was duped of Rs. 87,509 by a person, who called him claiming to be from the bank from where he had an account. The accused called the victim Shashank Raje, and said that he had his address and date of birth, and threatened that his card would be blocked if did not share his card number, pin etc. Raje shared his credits card number and there after he received an OTP, whose digits he shared with the accused. Police is yet to identify the caller.

ii. **Skimming** – It is theft of card's information using skimming devices during legitimate transactions such as purchases at alls, grocery markets or gas station etc. it is, thus illegal copying of information from magistrate strip of a credit card or debit card. Once fraudster gets hold of data, it can either be used for online purchaser with the details or they can forge a card with the data, known as cloned card and use that for over the counter transaction.[7]

In May, 2013 about Rs. 17 lakh was transferred from the personal account and it was done after the victim's mobile number in the bank's KYC form was changed by assessing it online. The person realized it when on May 6th, he received a call from the bank on his landline asking him to deposit some money in his account because a cheque issued for Rs. 4000/ was be dishonoured due to "*insufficient funds*" to the bank. When the victim examined his bank accounts details, then realized that Rs. 16,70,500/ was transferred from his account through RTGS transfer and net banking delivery channel on May 4, 2013. It is a case of theft of card's information using skimming devices during legitimate transactions, such as purchases at grocery market, gas stations etc.

iii. **Phishing** – A cyber offender obtains a consumer's financial personal information by sending him authentic looking e-mails.

Experts say that most of the victims of cyber crimes frauds are those who are working in senior positions in the private sector and also those who fall victim because of lack of awareness. According to the information available with RBI, the total monetary loss upto September 30, 2013 suffered by Indian was Rs. 54 crores and Rs. 48.46 crores upto November 30, 2013 respectively.[8] Although due to

growing instances and changing trends of cyber frauds, some banks send SMS often alerts to their customers asking them not respond or reply to false or suspicious mails or text message, yet it can effectively be checked by precautions, care and caution of customers. Twenty five nationalized banks of India have lost nearly Rs. 12,620 crores due to frauds in the last four financial years and there have been about 4,845 cases of bank's fraud over this year.[9]

Suggestions

The experts suggest the following precautions for computer users in order to check or minimize cyber frauds

a) Check the site properly before entering details.
b) Hide your CVV/ CVC numbers.
c) Check statements weekly.
d) Register for transaction alerts on mobile and e-mails.
e) Register for OTP.
f) Don't give your cards details to unsolicited callers.
g) Don't give photo-copy of the credit card to anyone without proper diligence.
h) Don't give your card along with its pin at shops, petrol pumps, hotel etc.
i) Don't save CVV/ CUC numbers as contact in phone-book of communication device.
j) Only use licensed software and browser.
k) Use one card online and another offline, set a transaction limit for cards used online.
l) Submit dispute resolution form to the bank within the specified time-frame.
m) Keep emergency numbers in hand to block the card, if necessity arises.

End Notes

1. Singh, P.K. (Dr.); *Laws on Cyber Crimes* (Book Enclave, Jaipur, 2000)
2. *Times of India*, Oct. 7, 2014.
3. *Times of India*, Jan. 13, 2015.
4. *Times of India*, Jan. 20, 2014
5. *Times of India*, Oct. 6, 2013
6. *Times of India*, Dec. 3, 2013.
7. *Times of India*, May 23, 2015.
8. *Times of India*, Oct. 18, 2013.
9. *Times of India*, Septt. 20, 2013

References

1. Singh, Pramod Kumar (Dr.)*;Laws on Cyber Crimes (Book Enclave, Jaipur)*
2. Jaga Rao, S. V. ; *Law of Cyber Crimes & Information Technology*, (Wadhwa & Company, Nagpur, 2004)
3. Kamath Nandan ; *Law Relating to Computer, Internet E-Commerce* (Universal Law publishing Co. Pvt. Ltd., Delhi, 2000)
4. Mittal D. P. *; Law of Information Technology (Cyber Law)*; (Taxman allied service Pvt. Ltd. Publishers, Delhi, 2000)
5. Rowland, Diana ; *Information Technology Law (2nd Edition)*; (Cavandish Publishing limited, London, 2000)