Perspectives in Science (2016) 8, 540—542

ScienceDirect

journal homepage: www.elsevier.com/pisc

Exploring and analyzing Internet crimes and their behaviours☆

Bhavna Arora

Central University of Jammu, Jammu, India

Received 20 February 2016; accepted 15 June 2016
Available online 5 July 2016

KEYWORDS
Cybercrime;
Cybercrime schemes;
Internet frauds

Summary The world today is experiencing an exponential growth in cyberspace. Nevertheless, India too has witnessed a significant ascend in Internet activities and it is quite assertive to say that such phenomenal growth in access to information on one hand leads to empowered individuals and organization and on the other hand also poses new challenges to government and citizens. To make the cyber world safe is the need of the hour. Putting up deterrent measures against cybercrime is essential to national cyber security in protecting critical infrastructure of the nation as well as for individuals. In this regard, the prime objective of the government is to prevent cyber attacks and to protect the country's critical infrastructure. It also focuses on reducing vulnerability to cyber attacks so as to reduce and minimize damage and recovery time. To prevent the cyber crimes, individuals and governments need to clearly understand the crime schemes in the cyberspace and the contemporary and continuing Internet trends and behaviours of these criminals. This paper gives a brief outline of categories of cybercrimes. These crimes are categorized as crimes against individuals, property, organizations and governments. Various Internet crime scheme are evaluated and behaviour of criminals to perform the cybercrimes has been analyzed. A critical evaluation of report of cybercrime complaints under IT Act 2000 has been presented.

Introduction

The rising rate of cybercrime with its varied and diverse characteristic features has been a source of concern. Cybercrime is a term that covers a broad scope of criminal activities by means of a computer. Cybercrime is referred to the act of performing criminal act using cyberspace as the communication medium (Harpreet, 2013). As a consequence of rapid globalization, low cost of mobile phones and easy access to Internet the cyber crime. The cybercrimes like cyber bullying and cyber defamation are common issues and are rapidly increasing. The government is framing policies and laws to prevent the growing number of such crimes. Most of the countries are not fully equipped with the legal infrastructure to handle cybercrimes. Young children

☆ This article belongs to the special issue on Engineering and Material Sciences.

E-mail address: bhavna.aroramakin@gmail.com

http://dx.doi.org/10.1016/j.pisc.2016.06.014

and youth are among the most targeted section of the society that is affected by the perilous effects of electronic media. Broadly, the cybercrimes can be of Type I and Type II. Type I cybercrime is generally a single event from the perspective of the victim. Type II cybercrimes, on the other hand refers to on-going series of events, involving repeated interactions with the target (Harpreet, 2013). These activities are such as computer related frauds, cyber defamation, cyber harassment, child predation, identity theft, extortion, travel scam, stock market manipulation, complex corporate espionage, planning or carrying out terrorist activities, health care, insurance/bonds frauds, auction frauds, fake escrow scams, blackmail, non-delivery of merchandize, newsgroup scams, credit card frauds, email spoofing, salami attacks, data didling, sabotage web jacking, spamming, DoS, software piracy, forgery etc.

Categories of cybercrimes

The role of computer in cybercrime can be classified in narrow or broad sense where computer can be used as an object, a tool or computer as the environment or context. The cybercrimes can be broadly classified as follows:

Cybercrime against individuals

In such cybercrimes, individual persons are affected. The goal is to exploit human weakness like greed and naivety. The potential harm of such a crime to humanity is severe. Few of the popular cybercrimes against persons include cyber porn specially child-pornography, violation of privacy, harassment of a person through e-mail spoofing, hacking, cracking, cyber stalking, defamation, cheating, fraud, e-mail spoofing, password sniffing, credit card frauds, gambling etc.

Cybercrime against property

The second category of cybercrimes is against property. Intellectual Property Crimes, cyber squatting, cyber vandalism, transmission of malware that disrupt functions of the system/wipe out data or create malfunctioning of the attached devices, cyber trespassing, Internet time thefts are few of the most popular cybercrimes against property.

Cybercrime against government/organizations/society

One of the distinct cybercrimes against government and related organizations is cyber terrorism. The individuals and groups use electronic media and the cyberspace to threaten the international governments and the citizens of a country. This crime manifests itself into terrorism when an government or military websites are hacked and vital information is retrieved. Cybercrime against organization and society mainly includes unauthorized access of computer, password sniffing, denial of service attacks, malware attacks, crimes emanating from usenet group, industrial spying/espionage, network intrusions, forgery, web-jacking etc.

Internet crime schemes

Today the current and ongoing Internet trends and schemes in the world can be categorized under the three classifications mentioned in ''Categories of cybercrimes'' section. People who carry out these crimes are called as cybercriminals. Depending on the motivation factor the cybercriminals can be classified as under (Nina Godbole):

Type I Cybercriminals — These include the hobby hackers or the politically motivated hackers who are hungry for recognition.

Type II Cybercriminals — They are not hungry for recognition. These include the psychological perverts, financially motivated hackers or organized criminals.

Type III Cybercriminals — These are the disgruntled or former employees seeking revenge.

Behaviours in cyber crimes

The cybercriminals mentioned in ''Internet crime schemes'' section track information in many ways. In this section, the behaviour of the cybercriminals to perform cybercrimes is outlined.

- In common fraud scams the criminals gathers the information by phishing and spoofing leading to identity theft. The imposter pretends to be the other person and uses their information without their knowledge to commit theft or fraud. Crimes related to health care, insurances are also performed by hacking and forging identities.
- Cyber harassment and defamation especially the cases of paedophiles and stalkers use false identities to trap the children and teenagers. Social media sites, chat rooms etc. are a major source for harassment and defamation.
- Cybercrimes like the electronic spamming is the abuse of e-messaging system to send unsolicited bulk messages indiscriminately. In this overheads like the lost productivity and frauds are borne by the public and Internet service providers, who are then forced to add extra capacity to cope up with the deluge (https://en.wikipedia.org/wiki/Spamming).
- In cases like the frauds like auction frauds, non-delivery of existent/non-existent merchandize, the seller responds to the victim of the auction fraud and poses to be in a region outside the place indicating emergency leaving (https://www.ic3.gov/crimeschemes.aspx). The criminal steals this information from certain unsecured websites or by identity theft.
- Forgery is often achieved by hacking wherein the hacker attack the target computer and retrieve personal information of the victims and use it for their personal monetary gains. The Industrial spying/espionage are achieved through ''spying''.

Cyber crime statistics

The Indian government has passed IT ACT 2000 which was amended in 2008 and focused on data privacy, information security, security practices, and inclusion of some additional cybercrimes like child pornography and cyber terrorism. In

Table 1 Summary of cyber crimes complaints during 2014 and 2015.

Cases type	Year	
	2014	2015
Economic		
1. Credit card fraud	9	14
2. ATM on line fraud	141	34
Face book		
3. Harassing/threatening complaints	24	23
4. Fake Facebook account complaints	46	35
5. Anti-religious complaints	6	—
6. Anti-national complaints	1	—
7. Hacked complaints	2	19
Mail		
8. Hacking/threatening complaints	2	3
Phone Calls		
9. Harassing/threatening complaints	3	2

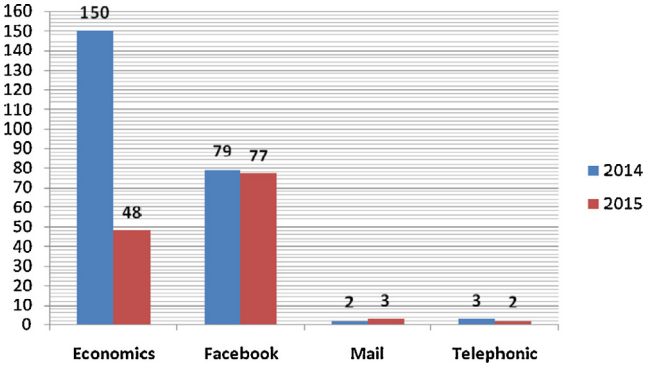

Figure 1 Comparison of no. of cyber crime complaints during 2014—2015.

this paper data is presented from the Cyber Cell Police Station of Jammu, Jammu & Kashmir, India. This cell was established in 2012. Table 1 shows the cybercrimes complaints registered during 2014—2015. The cases have been categorized under — Economics, Face book, Mail and Phone Calls

The graph presented in Fig. 1 gives the comparison on total number of complaints reported under the various categories — Economic, Facebook, Mail and Phone Calls in 2014 and 2015.

Analysis (Fig. 1): It is evident that the highest numbers of crimes are the ones that involve monetary frauds. The highest statistics that has been reported is 150 cases under the Economics frauds. However there are very few cases that have been reported under the mail and phone calls. The graph in Fig. 2 represents the percentage of variation in complaints registered in 2014 and 2015.

Analysis (Fig. 2): The graph indicates that out of the nine parameters under which the cases are registered, the perecentage variation of six parameter is negative. It implies that the cyber crime under six sub-citerias has declined.

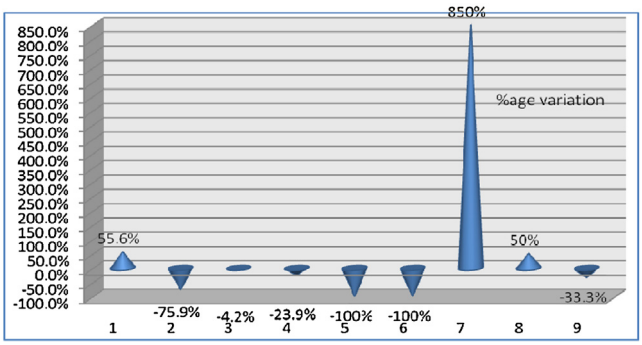

Figure 2 % age variation in no. of cyber crime complaints during 2014—2015.

However the percentage increased in three parameters cannot be ignored as well. The worst hit is the hacking complaints. There is about 850% increase in the hacking complaints.

Conlcusion

Information and communication technologies (ICTs); does not benefit to individuals, organizations and governments; but also widens the scope of criminal activities as well (Srivastava, 2012). Presently, the credit card thefts and online money-laundering cases of cyber crimes are on the rise. Harassment and defamation through social media are also a matter of concern to individuals. Cyber-terrorism is the most prominent aspects of cyber crime across countries. It is the lack of cyber crime awareness that leads to cyber-crimes. The Cabinet Committee on Security (CCS) approved the National Cyber Security Policy in July 2013 that aims to create a secure computing environment in the country and build capacities to strengthen the current set up with focus on manpower training.

Conflict of interest

None declared.

Acknowledgement

Sincere acknowledgement to the Cyber Crime Police Station, Jammu Tawi (J&K) for providing me data for this research.

References

Harpreet, S.D., et al., 2013. Cyber crime — a threat to persons, property, government and societies. Int. J. Adv. Res. Comput. Sci. Softw. Eng. Res. 3 (5 (May)), ISSN: 2277 128X.

Nina Godbole, Sunit Belapur, ''Cyber Security'', Wiley Publications.

Srivastava, S., 2012. Pessimistic side of information & communication technology: cyber bullying & legislature laws. Int. J. Adv. Comput. Sci. Technol. 1 (1 (November—December)), ISSN 2320 2602.