Cyber Crime – A Threat to Mankind

Charul Nigam*
Vaishali Singhal**

Abstract

Presently, the cyber space has become the most indispensable part connecting the man, business and life all over the globe. The number of connections & number of users being connected is increasing very rapidly, each year millions of new users are added to the network in various fields of internet such as social networking, online marketing etc. As fast as cyber space is spreading connecting man to man and business to business so is spreading "the world of cyber-crime." This paper discusses about the recent trends catching up in the Cyber Crime. It also focuses on the categorization and prevention measures of Cyber Crime.

Keywords: Cyber Crime, Cyber Space, Cyber Security, Hacking

I. Introduction

Cyber-crimes are being committed all over the world in various ways such as phishing, DOS attacks and Trojan attacks, email bombing and many more. Apart from this the cyber-crime also include criminal activities committed via internet such as online gambling, fake online sales of articles, theft of any sort of information present in electronic form, cyber defamation, unofficial access to computers etc. During the last decade a substantial growth has been observed in the cyber-crime failing all the several measures being adopted by different individuals and business organizations.

Although the term cyber-crime remains undefined by any justified decree still cyber-crime can be defined as the crime being committed using the computer system and network being used as the medium. Under this the computer system serves both as weapon and the affected victim. Cyber-crimes are being committed by various groups of individuals such as adolescents or children between 6 to 18 years of age group, various kinds of hackers (organized or professional) or discontented employees to name some. The reason behind the crime can be curiosity, business or revenge.

Charul Nigam*
Department of IT
Institute of Innovation in Technology & Management, New Delhi

Vaishali Singhal**
Student - BCA
Institute of Innovation in Technology and Management, New Delhi

Although mostly being committed purposefully there are still chances of accidents as connecting the whole globe together can't be a cent percent safe road.

Presently cyber space has emerged as a region where both optimistic and pessimistic ideas are developed, enhanced and escalated as soon as they emerge. People not only get influenced by these, but also become part and parcel of them. Cyber space has become a better half of social life of most individuals around the globe and when it comes to society both defeatist and affirmative constitutes the surroundings. While the affirmatives consist of tech-friendly users and professionals the defeatists consist of the "criminals of cyber world" Cyber space is considered as a public space by the offenders where one is free to do anything of his/her choice and do not consider their act as criminal. These offenders exist as old as the internet itself does and are also somewhere to be held responsible for the internet's present form. Cyber-criminals no longer consist of collegiate but also tech-savvy proficient who don't only have apprehension of all do's and don'ts but have also gained white-collar mastery of all the black jobs including blocking a website, posing obscene content(s), black marketing on the web etc. Unsurprisingly the cyber-criminal mostly constitutes the people among 15-34 years of age group.

Although it is practically indefinite to acknowledge how much a cyber-crime does cost they do have numerous monetary and non-monetary effects. While monetary forms include theft under online monetary transactions causing the loss of thousands or millions

and non-monetary may include spread of viruses in the form of applications or programs which may lead to the creation of botnets which can be further be used for the purpose of trafficking leading to the server failure of the host. By the elevating number of devices connecting to internet such as mobiles and tablets the exposure to cyber-crimes has increased several folds as the use of internet not only makes the device multi-tasking, but also provide multiple paths for crime to peek in. Out of all other cyber-crimes being committed theft of identity is considered to be one of the most dangerous in which the host grants the access to all the personal and confidential details including login, passwords, credential details related with online banking and business transactions.

II. History of Cyber Crime

The origin of cyber-crime goes back to 1960 when it started with the form of hacking. Hacking then evolved because of the activities committed by some MIT Model Train Engineers who revived the functioning of their model without actually re-engineering the model but by means of alteration of the source code of some early computers. Then in 1970 the hacking became evident, the hackers then known as phreakers developed codes that was capable of providing long distance service and embedded them in Bell Telephone Company in order to grab the personal information. This activity became a challenge for the legislation and evidence to the fact that the computer systems were a platform for the cyber-criminal activities as well.

The next cyber-crime was accounted in 1986 at Lawrence Berkeley national Laboratory where the malfunctioning of an accounting data was encountered. This was soon followed by the creation of Morris Worm virus by Robert Morris which resulted in the damage of around $98 million damaging 6000 computers and above. After this the legislation under Congress enforced acts and laws stating computer tampering a criminal and punishable offence.

III. Categorization of Cyber Crimes

In the present day, where cyber crimes are increasing day by day it has become strenuous to distinguish between a prevailing crime and a cyber crime. So as to make this demarcation feasible the cyber crime has been categorized as under:-

Against persons: These are the offences, which attempts to or actually vandalize the character of an individual. These are the crimes, which tend to degrade an individual's morale either socially, financially or psychologically. These crimes take place such as by communicating harassing messages, comments, videos, images or by stealing e-banking credential details etc through various means. These crimes intend to defame an individual by accrediting content, either which lower downs individuals dignity or tend to make business by theft in terms of hacking or cracking.

Against persons property: These are the crimes, which tend to harm person's possessions in particular. These

Fig. 1: Categories of Cyber Crime

crimes generally come into picture because of the global enhancement of merchandising on the internet. Today both buyer and supplier are frequently making their hand to make business through internet thus leading to huge amount of data being stipulated on internet thus making pace for unauthentic access very common.

Many cases occur where domain names become inaccessible by the use of multiple users claiming the name to be registered either by them based on their registration priority or by accessing the same name. Crime also comes in when the user's data on the network has intentionally been tempered to cause business failures. Hacking is one of the crucial crimes under this head. Hacking can take multiple forms such as time-theft (which occurs in the case when the charges of internet services are taken on hourly basis), cyber-trespassing (in this case no harm to the device or data is caused but is used unauthentic ally by non-permissible means such as connecting to Wi-fi without its owner's permission) etc.

Against government: These are the offences done in order to hamper global peace and harmony by means of internet. These are of various forms such as cyber-terrorism (It is a matter of native and worldwide distresses, in this the jurisdiction and nobility of a state is exposed to danger.), cyber-warfare (It is a purposefully done militant act done for the sake of obstruction and counter-intelligence; form of hacking) etc. Internet has made information easily accessible for terrorists, which they use as a weapon for their civic, theological and communal aims.

Against society: Any illicit activity done with the objective to molest the network can be vulnerable to many users. These include both financial and non-financial offences. The financial offences include online gambling (these include different types of gambling offered online such as bingo, poker, casinos, lotteries etc; all these are offensive means of making money) and other financial crimes such as credit card and debit card frauds.

IV. Recent on Cyber Crime

Pakistan based group suspected for hacking revenue based website: Pakistan based group is suspected for hacking the web portal belonging to Income tax department under Indian Revenue service (IRS). The officials reported that the website has become inaccessible from Feb. 7 2016 leading to failure of communication between the central board of direct taxes and the IT department field office. The website had slogans promoting Pakistan territories have been reported by the officials accessing the website.

Japan, Singapore, Malaysia & India sign pacts for cyber security: Three pacts have been signed between Indian computer response team(CERN-In) and its analogue in Japan, Malaysia and Singapore on accounts of Cyber security. The pact was framed and sealed firstly under PM Narendra Modi's trip to Malaysia in November 2015. This pact will focus on enhancement, development and enforcement of techniques and ideas amongst the three nations to boost cyber security.

Cyber criminals nagged from Kolkata: Three former employees stole the credentials of UK based clients and assaulted money on account of technical assistance into the account faking to be on the firm's name. The trio maintained the directory for such prey's using the cloud addressing from where the data was later on downloaded through PDA's and money extracted was shared between the three.

UK police campaign's for young hackers: A survey reported that the average cybercriminal age has turned down to 17 thus the Britain's National Crime Agency has started a campaign aiming to be an alarm for parents of boys belonging to the age group of 12-15 that they should become alert keep an eye on the activities being committed by the youngsters around them as they can turn out to be young criminals in disguise.

900 hackers nagged down by China: After being criticized by the US over inflated cyber attacks by Chinese criminals intending American firms. China has nagged down 900 hackers under their online campaign. Most of those arrested already posed to have a criminal background.

Cyber Crimes to be checked through reporting helpline: A free online helpline has been launched in Delhi-

NCR for reporting cyber-crimes. After the helpline became functional more than 250 cases had been lodged in around a fortnight. Considering all the cases phishing and money-laundering were mostly reported followed by women harassment.

Above 100 million Indians dissipated around Rs. 16000 on cyber-crime: Nortan software security firm reported that around 100 million and above Indians have dissipated Rs.16000 on account of cyber-crime and suffered social, emotional and financial harassment. As per the nortan report the users of age group 55 and above considered as less tech-friendly have been to abide more cyber secure habits than the young & more tech-friendly users.

More than 70 percent Indian firms duped by Cyber attacks: A survey report concluded that more than 70 percent Indian firms have been duped by cyber attacks in year 2015. Cyber-attacks were considered to be most harmful for the corporate by about 94% said the report.

Over 125,000 profiles suspended by twitter: Twitter Inc. had reported that from 2015 onwards 125,000 profiles had been suspended which seemed to promote anti-socialism and terrorism especially related to ISIS.

VI. Prevention Of Cyber Crime

Safe-guard your device: If the device is not properly secured then it is prone to be hampered by the offenders or the offenders can get the access to your credentials on the basis of your device. Always get the latest and authentic security software for your device and do keep them fully updated. Must get your device firewall protected.

Have a safe "site": Be always sure about the links you visit. Always go for safe and familiar links. Do not just blindly follow hyper-links whether they are from emails, profiles or blogs these can be either malicious or fake copies of original one's leading you to a dangerous situation.

Obviate "yourself": It is highly recommended that one should never send his/her personal details through emails as in such cases the chances of cyber-attacks are highly rated. Authorized corporate never demand personal details through emails.

Have compelling passwords: Several software has been programmed having the capability to suspect the passwords. Passwords should be such that they are "hard to crack but easy to grasp". Always make long passwords of mixed cases that is, including both lower and upper cases. Passwords preferably should be mixtures of characters, digits and symbols. It is endorsed to make multiple passwords for multiple accounts.

Protect Yourself: By means of search engines one can easily track other's public information. It is a suggested practice to set your search names difficult. The data provided by the data service providers is not guaranteed to be secured due to their complexity in terms of number of records and the compilation of data from diverse sources and thus there are chances of your public information being used by the offenders for their intended and harmful use.

Limit your data: Always make sure to remove the data from your profile as well from other's profile relating to you and that is under your control once it becomes unwanted for you as it can become a threat in future. It would be rather a safer practice to avoid posting privileged information in the first place.

Do review your accounts: Mostly there are three options available on social networking accounts update privacy settings, delete the data or delete the account. If you ever go for deletion of your account always do make sure to delete all your data first. Always prefer for deletion of your account rather than deactivation.

Communicate cautiously: While communicating on internet being sure is highly unsure. Always cross check all your communications even those claiming to be trustworthy. Go for links which you are sure about or are familiar with in case of any doubt do not go for it at all.

Avoid Spams: Do not respond or reply to any spams as they are surely harmful.

Prevention is better than cure: Spotting of vulnerabilities will help associated firms and corporate deal with these challenges.

Avoid pop-up: Never give any credentials as input in any pop-up advertisements. If you want to go for the deals offered by means of pop-ups always contact the dealer by either going to the authentic websites or homepages and not by the links provided on the pop-ups or by any other permissible means.

Keep photographs in safe: due to increased pornography cases, it is recommended to avoid sharing of photographs amongst strangers online.

Keep a careful watch: For underage or less tech-friendly users parents guidance is an advisory in order to prevent future aggravation for children.

VII. Conclusion

Due to the multiplying number of computers and users of internet all around the globe and ease of accessibility of resources by means of internet in fraction of seconds the security has become a major issue of concern. It is neither simple nor practicable to abolish cyber-crime in a single go due to all technological enlargements. Although there is a scope to withstand and scrutinize the cyber-crimes. In order to gain this objective first the users worldwide should be made capable to identify such crimes, made to learn secure and safer tech practices and prevent such offences.

References

1. http://cyberlaws.net/cyberindia/articles.htm
2. http://satheeshgnair.blogspot.com/2009/06/selected-case- studies-oncyber- crime.html
3. http://www.legalindia.com/cyber-crimes-and-the-law/
4. http://www.ibnlive.com/newstopics/cyber-crime.html
5. www.indiancybersecurity.com/.../8_history_of_ cyber_law_in_india.htm