THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Cyber Crime: Impact and Investigation Process

[1]Ms Upasana Sharma and [2]Ms.Harinder Kaur

[1] Student, Department of Forensic Science, School of Bio-engineering and Biosciences, Lovely Professional University, Phagwara, Punjab, India

[2]Ms. Assistant Professor, Department of Forensic Science, School of Bio-engineering and Biosciences, Lovely Professional University, Phagwara, Punjab, India

Corresponding Author: Ms.HarinderKaur

Email id: kaurharinderheer@gmail.com

Contact No.- +919530626972

ABSTRACT

Cyber-Forensics is the combination of two sciences; one is Information Technology and second is Forensic science. Now-a-days humans are able to access everything from their house via internet. Information Technology provides a lot of benefits to the humans but it also has the capability to lead them to vulnerable situation if they are not aware about the loopholes which they left behind. Most of the population have no idea about all these crimes & how to get rid of it. This paper will create general awareness about cybercrime, its types, preventive measure, and procedure of investigation etc. among the general population so that the concept of cybercrime is easy to understand.

Keywords- Forensics, Cybercrime, crime investigation, information technology, cyber security

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Introduction

Humans and crime shares very strong bond from the centuries [1]. Earlier the techniques for committing crime were different but today crime is also up to date. In this era, humans are fully dependent on technology, from sending mails to washing clothes [2]. Now internet is being used as the advanced technology for the communication and information exchange medium. On the daily basis technology is getting advanced which is beneficial & proud event but whenever new creation happens there is antonym of creation that means destruction also comes. In this era, IT field is very dominating field among the people. From shopping, bill payment, transactions, gathering knowledge; everything is connected with computer via internet and this computer is transforming creation in IT sector. But every coin has two faces; one side if computer saves our time & energy; on the other hand some are using it for committing heinous crime. With the help of internet & computer technology one person can destruct another person's life on commercial, physical & mental basis, because hackers use person's personal information against them. So it is necessary to get aware about the cyber world so that a person can protect themselves from the frauds. If people don't put themselves in vulnerable situation or left loopholes behind them no one can take advantage of them [3]. So, it is necessary that everyone should know the concept of cyber crime & their preventive measures[4] .

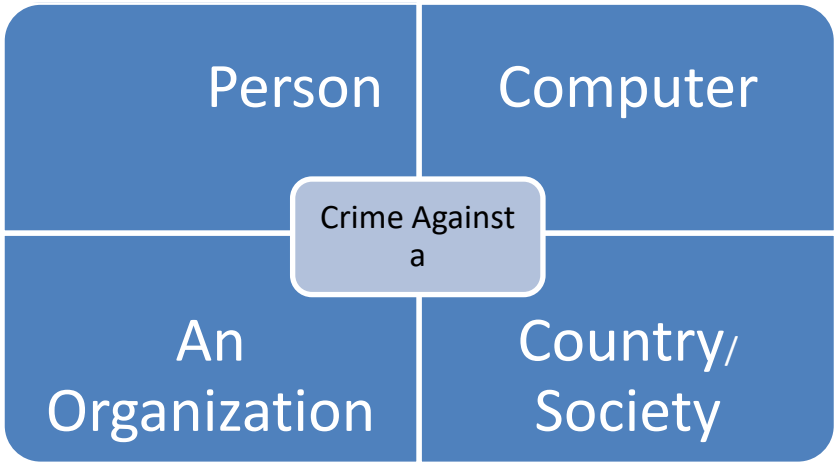
Definition of crime: From Indian Context; Crime is defined as an activity that involves breaking the law & enforcement [5].

Definition of Cyber Crime: Cyber-crime is an unlawful action in which either a computer is a prey or a person [6].

Types of cyber crime

Cybercrime is that crime in which computer is used as a tool to commit a crime against something or sometimes it would also become a target. On that basis it is classified into following categories:

ISSN: 0971-1260
Vol-22-Issue-17-September-2019



Crime against a person: In this case, target is a person, following crimes comes under this classification;

1. Child Pornography: possessing, circulating or formation of obscene images or videos of a juvenile, it comes under child pornography.
2. Cyber stalking: this is an act of stalking, harassing or threatening a person by means of internet via mails or messages.
3. Forgery & Counterfeiting: forgery & counterfeiting of document with the help of advance tools & techniques, so that no one can recognize the document without the help of professionals.
4. Money Frauds: a person may deduct money from another person's account by gathering the information of credit card, debit card, PIN, OTP details.
5. Phishing: gathering personal & sensitive information of an individual like credit card & debit card PIN, OTP etc. by masquerading mails.

Crime against a computer: When the target is a computer, following crimes comes under this classification;

1. Hacking: in this particular crime, people get access of another person's computer for sake of stealing, modifying or destroying sensitive information present in the computer.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

2. Data diddling: before processing a computer criminal alters the crude data & then changes it back after the completion of processing. It's like manipulation of input.
3. Key loggers: with the help of an key loggers one person keeps an eye on another person's computer like what they are searching, at what time they are using it etc.
4. Transferring viruses/worms: a person sends viruses & worms to another person's computer to slow down or affect another's computer.
5. Malwares: The malicious program are designed or installed to gain access of another person's computer eg. SPYWARE, TROJAN HORSE etc. this is harmful for the computer in which it is installed but it is beneficial for the 3rd person.
6. Spamming: sending junk mails via internet so that it should decrease the storage space for other files.

Crime against an organization: When rival company & or an individual who wants to destroy a company commit crime by means of computer or internet. Under this classification following crimes comes up;

1. Denial of service attack: cyber-attack, network of particular website got collapsed by flooding it with useless traffic. Everything will shows up, but you can't access it [7].
2. Online Auction Fraud: Many genuine websites offers online auction but some cyber criminals take advantage & frames fake online auction for some target company.
3. Web jacking: Cyber-criminal gain access of an organization's website & modify the content, post obscene contents or block the website and due to this act, an organization may face a lot of loss.

Crime against a country or society: society or a country is harmed by cyber criminals;

- Cyber Terrorism: spreading of terrorist activity or content which provoke public to do an act which harms a country or society. [6,8].

Impact of Cyber Crime

- First thing which got affected by this crime is goodwill. If any reputed organization faces hacking, phishing like crimes then for some period its reputation got affected.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

- Financial loss is the second impact of cybercrime.
- Fearful Society builds up by cyber terrorism.
- Economic growth of the country got affected by this.
- Cashless transaction idea got affected as crime can creates fear in people's mind [9].
- Suicide rate may also increase because of cyber bullying, stalking, pornography etc [3].

Laws under IT Act 2000

Information Technology Act 2000 (IT ACT) (India) covers certain offences & the punishment related to information technology crimes. Some common laws which come under IT Act are tabulated below:

Categories of cyber criminal activity	Computer related crimes like Hacking, sending malwares, viruses or any kind of destructive activity of computer or its source.	Obscenity in electronic form (Pornography, Child pornography)	Non Compliance of directions, cyber terrorism etc. (including cyber security	Breech of confidentiality, privacy etc.	Offences related to Electronic Signature Certificate
Sections under IPC	65, 66, 66B, 66C & 66D.	66E, 67, 67A & 67B.	66F, 67C, 68, 69, 69A, 69B,	72, 72A, also 66, 66B, 66C, & 66D	71, 73 & 74

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

			70& 70B.		
Who is the victim?	Person	Person	Nation or society	Person	Person

[10]

Procedure for investigating a cyber crime: It is easier to apprehend the criminal before the commission of any other criminal activity if the previously committed crime has been detected by investigators. For this there is a branch of science that is known as forensic science. Forensic science deals with collection, preservation & analysis of evidences which are related to the case. During the investigation of cybercrimes, digital evidences like pen drive, laptop, hard drive, floppy etc. are collected to retrieve some kind of information.

There are the 5 structural steps which are followed by forensic team:

1. Identification & Acquisition of digital evidences: at the crime scene a number of items may present but it is the duty of examiner to identify the evidences which are relevant to the crime. In digital crimes computer, laptop, pen drives, floppy, CDs, memory card etc. are the common evidences through which information can be gathered related to the case.
2. Preservation of digital evidences: the digital evidences are volatile (can be erased easily) in nature. So the digital evidences are always packed in faraday bags which stop the connection of digital evidences with other waves.
3. Analysis of digital evidences: there is an idiom that "Diamonds cuts Diamonds" similarly if computer or internet is used for commencement of crime then usage of some special software for the analysis of evidences is necessary. In analysis section main point is to make a copy of the data which is present in suspect's computer because examiner has to examine the data on copied form so that original evidences should not be demolished. Some common softwareswhich are used in solving crime is ENCase, SANS SIFT, CAINE, FTK Toolkit, The Sleuth Kit, Volatility, Bulk Extractor, Xplico, Oxygen forensic Suite etc [11].
   The software is used to recover deleted data, to check volatile memory of system, check disk imaging etc. All these software are used to get the information precisely.
4. Make a Report: after analysis of the evidences next step is to make a report on whatever the evidences found and performed examination related to the case.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

5. Presentation of the report: making report is not enough; examiner has to be present in court while hearing because his testimony is important. Sometimes terms used in report are not in layman language then the presence of examiner make it easier to understand the details written in report

In short; cyber forensic team play a very sensitive role in investigation because their one mistake or negligence results in destruction of the evidences & make the simple case complicated which leads to injustice that is a bigger crime than any crime.[12]

Cyber Security

Cyber security means to secure the data, information or system from unauthorized access, any kind of alteration or destruction. There are 3 elements of information security system;

a. Confidentiality: it means to keep the private or sensitive information hidden so that untrusted authorities can't access the information.
b. Integrity: always maintain the accuracy of data in its life cycle & protect it from unwanted modification from unwanted source.
c. Availability: ensure that all the hardware are working properly or give the maintenance to them after sometime so that whenever person want to access it is available to that particular person.[13]

Cyber Crime Preventive Measures

- Always use strong passwords so that, it become difficult to hack your account or device. Eg. Use a "passphrase" which means password having a combination of upper & lower case letters, numerical, capital & small alphabet; like if any person's name called Ranveer & whose birth date is 29 then can make a password like $R@nveer29.
- Don't click on any mail or links which comes from unknown or untrusted source because after clicking on these viruses, malwares or worms which are attached to the mail get installed in your device [14] .
- Do not post every single detail about yourself on social media because now-a-days social media also serves as a good source to obtain information about a person [15].

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

- Do not enter or share your sensitive information regarding your bank account, card details, ATM pin etc. on unknown websites [3].
- Always Use latest / advanced Antivirus software to protect your device
- Avoid using any public avail Wi-Fi because it is harmful & at the same time hacking is easier for the hackers.
- Banks won't ask A/C detail of their customers including account number, ATM card details, password etc. by sending messages or mails; if any mails or message comes to your account then it must be a phishing attack. So be careful while sending sensitive information.
- Always check your bank transaction if any kind of suspicious transaction seen then immediately report it to the bank [15].
- Don't save your passwords in your laptop or mobiles if a person hack your one device automatically that can access your other devices without any special effort.
- Don't keep "Remember Password" button active for your accounts [16].
- Last but not the least point; always report to cyber cell, if any kind of cybercrime occurs because your negligence leads to serious crimes.

REFERENCES:

1. AmitWadhwa and Neerja Arora, "A Review on Cyber Crime- Major Threats and Solutions". International Journal of Advanced Research in Computer Science. vol. 8, No. 5, 2017
2. Preeti and Sushil, "Tool and Techniques for Computer Forensics". 4th International conference on System Modeling & Advancement in Research Trends, 2015.
3. Shweta Ghate & Pragyesh Kumar Agrawal, "A Literature Review on Cyber Security in Indian Context". Journal of Computer & Information Technology. Vol. 8(5), 30-36, 2017.
4. G.Nikhita Reddy, G.J. Ugander Reddy, "A Study of Cyber Security Challenges and Its Emerging Trends On Latest Technologies". International Journal of Engineering and Technology. Vol.4 No. 1, 2014.
5. Ratanlal and Dhirajlal, " Indian Penal Code".Lexis Nexis, 2013.
6. Prof. N.V. Paranjape, "Book – Criminology, Victimology & Penology". Central Law Publication. 2017 ed. 2017.
7. Jitendra Jain and Dr. Parashu Ram Pal, "A Recent Study over Cyber Security & Its Elements". International Journal of Advanced Research in Computer Science. Vol.8. No. 3, 2017.
8. https://swayam.gov.inhttps://youtu.be/sBk4Nn5jflU

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

9. Hemraj Saini, Yerra Shankar Rao and T.C.Panda, "Cyber-Crimes and their Impacts: A Review". International journal of Engineering Research and Applications.Vol. 2. Issue 2. pp. 202-209, 2012.
10. Vakul Sharma, "Book - Information Technology Law & Practice". Universal Law Publishing. 3rd ed., 2011.
11. B. V. Prasanthi, "Cyber Forensic Tools: A Review". International Journal of Emerging Trends and Technology. Vol 41 No 5, 2016
12. Richard Saferstein, "Forensic science: from the crime scene to the crime lab" . Pearson. 3rd ed. , 2016.
13. Hardik Runwal and Pooja Akulwar, "A Survey on: Cyber Crime & Information Security". IOSR Journal of Computer Engineering. Vol. 20, Issue 1, PP 30-34, 2018.
14. G.Balaji, V.S.Hari Prassath, V.Sriram, "Issues Based on Cyber Crime and Security". International Conference on New Horizons in Science, Engineering and Management and Humanities, 2018.
15. Rajarshi Rai Choudhury, Somnath Basak, Digbijay Guha, "Cyber Crimes- Challenges & Solutions, "International Journal of Computer Science and Information Technologies. Vol. 4(5), pp 729-732, 2015.
16. Monalisa Hati, "Cyber Crime: A Threat to the Nation and its Awareness". International Journal of Advanced Research in Computer and Communication engineering. Vol. 5, Issue 7, 2016.