To Study The Causes And Protection Of Cyber-Crime: Theoritical Frame Works In Over All Nation

Dr. S. Muthukumaravel, Rufus Sooria Kumar, Dr. N. Purusothaman

Abstract: A general notion about crime and its offences to others may lead to the understanding of murder, rape, theft, robbery, kidnapping, threatening, outlaw, extortion and dacoit. There is more danger in cyber-crime when it is compared and already discussed in the above line. The cyber-crime takes plays fully on the internet connection and with the network system. The internet connection has cyber space in network. It contains both good and bad information. But few people select the bad content and use the cyber space criminally. Since, the cyber-crime takes place in network space, and hence this article attempts to read the Meaning, Types, Causes and Protection of cyber-crime in nationwide theoretical frame work.

Index Terms: Cyber-crime, Cyber Space, Crime and its Offences, Causes & Protection.

1 INTRODUCTION

THE effect of cyber-crime is not only in India, it affects worldwide. In the world best efforts are taken to avoid the offences and control the cyber-crime. But it's not possible to control and avoid completely. The reason is that world leaders are not united to fight for the cause. The leader of a particular country tries to secure the problem with other particular country. The world leaders should discuss and agree to sort out the differences and take concrete measures to eradicate cyber-crime. Otherwise it is an ongoing process. In History of cyber-crime the first spam email took place in 1976. When it was sent out over the ARPANT and the first Virus was installed on an Apple computer in 1982. It was done by a high school student Rich Skrenta who developed the EIK Cloner.

1.1 OBJECT OF THE STUDY:

a) To study the Cyber-crime in the Global Environment.
b) To know the Causes of Cyber-crime.
c) To create Awareness of protection from cyber-crime.
d) To find out the solution of cyber-crime to the public.

2. Review of Literature

Higgins[1] (2010) concludes that technological advancement has led to security issues over the internet. The criminals have developed their own strategies and cyber knowledge to hack the systems and download critical data. Criminals in turn use the information to black mail corporate and individuals worldwide. Higgins concludes that cyber crime is highly vulnerable affecting the individuals and corporate globally. Cyber crime can be controlled through in-depth knowledge on internet technologies and constantly protecting cyber crime through fire walls and Legal system.

Welsh[2] (2011) has coined today's generation as "digital natives" or the "I- Generation" totally dependent on technology. Today's generation is completely connected on line 24/7 for various networking and using for social media. It has affected their psychology, thinking, attitudes and towards the society. Many are addict to their electronic gadgets and misuse the technologies resulting in failure of achieving greater objectives in life. As adolescents they try new technologies or websites which pollutes their mind and unprotected from privacy. Das and Sahoo[3] (2011) observes that social networking sites cannot be demarcated. Individual's data are not protected nor their privacy. Technology or social media websites like Facebook can locate a person's physical presence. It also affects the psychology of the individuals entering the world of virtual relationships. The habit of using social media daily and the hours spent on the internet has affected productivity and health. Social media has been misused in spreading fake news and instigating people to agitate and rise against the societies and governments. This has led to huge loss of life and property. The author has not stated the measures to be taken to control cyber crime. Vadhera[4] (2012) observes that social networking sites have become new battle grounds to enforce opinions and decisions. It helps them to target and manipulate information for vested interests. The Governments assurance and actions has not minimized the social media. Cyber laws are inadequate to bring the social media under control. As there are many players in the social media from different nations governed by their countries of law. The legal disputes have been increasing at a galloping rate for the crimes on-line. Chandra[5] (2013) highlights the vulnerability of young children who are connected to the social media. Children end up being bullied or induced to commit crimes. Many parents have hard times for their children being stalked. The parents are in a dilemma. Children being tech savvy will help their education and job prospects. It may also misguide the children to be trapped in cyber crime.

3. CAUSES OF CYBER-CRIME:

The criminal always thinks how to get more money in an easy way especially in cyber-crimes. So he chooses this way. Generally what we think about cyber-crime is that people cheat the rich people and thus collect money. But the cyber criminals want more money in easy way so they target not

- *Dr. S. Muthukumaravel, Assistant Professor, Patrician College of Arts & Science, India, E-mail: muthukumaravels1980@gmail.com.*
- *Rufus Sooria Kumar, Assistant Professor, Patrician College of Arts & Science, India, E-mail: rufusga@yahoo.com.*
- *Dr. N. Purusothaman, Assistant Professor, Patrician College of Arts & Science, India, E-mail: purusoth051986@gmail.com.*

only rich people; they select each and every individual. But their concentration is on rich people. The cyber criminals are monitoring user's transactions in the system. Hackers study the purpose and pattern of people using systems in continuous manner. After few days the criminals easily cheat the normal people. To trap such cyber criminals is a difficult task. In this process cyber-crime flourishes around the world. Computer users are vulnerable ones, so laws are required to protect and safeguard to the normal people from cyber criminals. The followings state the reason for the vulnerability computer users.

3.1 Easy to access:

The cyber criminals have mastered the hacking system for computer access. So it is easy to access the common people and their network systems right in his place. The criminals easily hack and cheat computer users. It may look like access code, thumb impression and voice recorder. Hence, they can cheat biometric system also.

3.2 Storage Capacity is very small:

The space of computer has small storage capacity for the data storage. Hence, the cyber criminal uses this drawback and collects the information from common people's data from their computer easily.

3.3 Complex:

The computer required on operating systems and these operating systems are programmed with millions of codes. Our system operators cannot memorize these codes in his mind, so the mistake will be natural. Hence the cyber criminals misuse their mistake and to commit cyber-crime.

3.4 Negligence:

Negligence is the one of the characteristic of human being. It is the system operator's negligence to protect the computer form virus and hackers. It is unconsciously a welcome for cyber criminals to access and control the computer systems.

3.5 Loss of Evidence:

It is easy for the cyber criminals to destroy the criminal evidence in computer. So we can't trace when, where and who has committed the cyber-crime. This is a great advantage for cyber criminals to cheat the normal people and one can easily escape from the problem.

4. TYPES OF CYBER-CRIMES:

4.1 Hacking:

The cyber criminals have advance software's for hacking, collecting or stealing the data from normal persons. Hence, the cyber criminals are called as Hackers. We can't trace the Hackers website and their place because they have advanced software. The hackers are equipped persons in the concerned field. The hacker's primary target is Government portal information. The secondary target is normal individuals with good financial status. The hackers illegally access into the data from remote location. The government as initiated to take more effective security measures to control some extent. Hackers are hacking data consciously. Hence it is hard to stop this crime.

4.2 Child Abuse and pornography:

The cyber criminals hack through the website to abuse children by showing pornography. When the children are playing games in computer system or android cell phones the criminals are sending chats that looks like opposite gender. The children reply the chat and they get pornography message, photos and videos. This is also criminal activity by corrupting children's mind. Most of the parents are fully occupied in their work so they could not monitor what their children are doing in their system. The ultimate goal of cyber criminals is how to spoil the children's life and leading the children in wrong way.

4.3 Theft of privacy:

The normal people are using unauthorized website and downloading some data like game, photos and videos. This gives an opportunity to the hackers to hack the normal persons systems by sending virus. By this the hacker can easily collect data from the normal persons systems. The hackers also target movie producers by uploading the movie online and demanding ransom. The full movie is uploaded first in the computer before the date of releasing the movie in theater.

4.4 Cyber Terrorism:

The cyber terrorism is totally different form cyber-attack. The cyber attacker's motive is to collect the information illegally and their main motive is money from the normal people especially from famous individuals. The cyber terrorism is not only collecting information and money from the famous people but the main motive of cyber terrorism is to fully destroy or to damage the important data from the government organization. The cyber criminals are creating a feel of terror in the mind of the victims. So the ultimate motive of cyber terrorism is to create fear in victim's minds.

4.5 Theft of Identity:

The cyber criminals hack each and every individual's identity from the computer. The system users are using internet mainly for cash transaction, online purchasing and banking services. They steal information from common people. The information is like individual details of debit card, credit card and some important data. The cyber criminals get the money and things from the individual identity. The ultimate goal of cyber criminals is to create major financial losses for the victims and spoil the victim's credit scores.

4.6 Computer Vandalism:

The computer vandalism is different from virus. They attach themselves to existing program. The main motive of this theft is to create a harmful program. The aim is to erasing the data in the hard drive. The process is by extracting login credentials. The business competitors are doing this type of criminal activities to jeopardize their competitors.

4.7 Malicious Software:

This software is programmed for the internet software. This virus creates disturbance in the network. This software is used for gain access of computer and steals the sensitive information or data and thus causes the damage.

5. PROTECT FROM THE CYBER-CRIME:

It is for establishing multidimensional collaboration between public and private sector. By passing law enforcement, information security organization, information technology industry, internet companies and financial institution are well protected.

5.1 Highly Secured Password:

Using strong password for online transaction can protect the cyber-crime. In this way it is easy to avoid cyber-crime problems. The weak password can be easily hacked by the cyber criminals and they easily access our data. The password is very important aspect for the access the online transaction so the password must combination of special character, numerical and alphabets. **Example:**Arulscott@1997or Arul@scott_1997.

5.2 Do not reveal it to others:

The strong password must be the most important and the similar to the earlier of the user. They are not supposed to tell the password to others. This is also an important aspect for avoiding the cyber-crime. The user knows only the password and access the data. To store the password in memory or keep note in separately is an essential aspect in this case. The user may have an important work or circumstance but at the time he/she shouldn't tell the password to others.

5.3 Data Protection:

Protect our data very safely is like protecting our financial information, taxpaying, and personal information. Data protection has to be safely maintained in a correct manner

5.4 Protection required for Computer system:

Fire wall software's protection is required for online security. The user continually updates the computer system with the help of security software. High security software includes firewall and antivirus. Firewall is called as computers' first line of "defense" and it looks like policeman. In order to control it the unauthorized person enters the individual system.

5.5 Information of Social Media:

Don't put unnecessary information to social media like Face book, Whatsapp, Twitter and You Tube. When you are posting the information in the social media one has to think more than one time and then post you information into the online. Unnecessary information may create more problems; this information is helpful for cyber criminals.

5.6 Identity Protection:

Identity can be considered as our personal details like name, address, contact number, unique numbers and financial information. This information is very useful for cyber criminals. So this information should be very confidential and shouldn't reveal it to others. If one reveals this information to others may lead into unavoidable circumstances. The online website has to be secured domain and has to maintain our information in high security. Thereafter one can share his personal information to any other website. Don't give your personal information to all website holders. The cyber criminals can easily track our personal information when we put unnecessarily our data to an unsecure website.

5.7 Security required for Mobile Phones:

Most of the people are not aware of cyber criminals and their hacking of information from cell phone. In same manner they are hacking and the details from our computer. So high security software like antivirus and secure lock screen is needed for the protection of our system. The updated operating software for mobile phones is necessary one. The hackers easily collect our information from cell phone when our mobile is not secure.

6. CONCLUSION:

The cyber criminals are collecting and hacking the information from rich and famous individuals. Their motive is to earn more money in an illegal manner. This is the reason that the cyber criminals are choosing this cyber-crime. The Government organization and private organization cannot stop or control the cyber-crime. The above mentioned details are the responsibility of each and every person. Each and every person knows very well about the software and its details or at least high security software in his computer and cell phones needs to be installed. Users must update the security software. They maintain updated operating software; they are using their computers or cell phones. At anytime an unauthorized person should not chat with him and block at the time. We are using mobile phones thus we can avoid unnecessary searching in portals and collecting information from that particular website. Don not switch on the location mode while internet data is switched on in your cell phone. These are the basic lessons to be followed. Thus, it has to be begun with each and every one then only we can control the cyber-crime. Otherwise, it will be an unending problem of the tale.

REFERENCES

[1] Higgins and George, 'Cybercrime: An Introduction to an Emerging Phenomenon", McGraw Hill Publishing, New York 2010.

[2] Welsh and Jennifer, "Is Constant 'Facebooking' Bad for Teens? Live science", 6 Aug. 2011.

[3] Das, Biswajet, Saho and Jyoti, "Social Networking Sites. A Critical Analysis of its impact on Personal and Social life", International Journal of Business and Social Science, Vol.2 (14) 2011

[4] Vadhera and Sharad, "Fate of Social Networking Sites in India", Kan and Krishme, Global Advertising Lawyers Alliance 2012.

[5] Chandra and Neetu, "Social Networking sites a concern for Parents", India Today, April 1, 2013.

[6] Sudhansu Bhushan Roy "Essay on cyber crime in online article" April'18.