ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 4, Issue 4, pp: (599-607), Month: October - December 2016, Available at: www.researchpublish.com

A SOCIOLOGICAL STUDY OF DIFFERENT TYPES OF CYBER CRIME

Dr. Grace Varghese

MA, MPhil, PhD, Pullannivelical House Mylapra Town P.O Pathanamthitta Dist Kerala, India.

Abstract: **Information Technology has made revolutionary changes in the dissemination of information and knowledge. On line transactions on banking, reservation of tickets, downloading of certificates, procurement of goods and services, electronic mails are advantageous and save time, energy and money. But with the increase in the use of computers, internet and mobile phones in our daily life, there is also a corresponding increase in Cybercrimes. In spite of very high punishments prescribed by law, such crimes are on the rise. Cybercrime is the deadliest type of crime. It can disturb existing set-up within the fraction of a second. Thus, Cyber criminality has potentiality to show its effect across the globe. The problem of Cybercrime can be understood by understanding Cyber technology. The world is witnessing the situation of ever growing field of Cyber technology. The technological growth rate is too fast. In last decade itself, the number of citizens increased by 100% in India. Technological adoption is at its peak. However, the problem of Cyber criminality oozing out of technological adoption is not properly tackled along the line of its growth. Thus, the period has been witnessing the different pace of development between Cyber technology and infrastructure in preventing Cybercrime. Within a short span of decades, a huge gap between Cyber technology and Cyber criminality has happened without any hope of bridging the gap.**

Keywords: **Information technology, Cyber crime, Growth, Globe, Law.**

1. INTRODUCTION

A common man who is a user of computer and internet and cell phone is unaware of the traps set by clever criminals in the Cyber space and the ways to get rid of them. Computers evolved as a result of man's search for fast and accurate calculating devices. Forging documents is one of the best examples of this kind of a Cybercrime. Image morphing, circulation of defamatory comments and threats through mobile phones, taking photographs without consent and consistent blackmailing may be some other examples. With the rise in the internet users Cyber criminals are also increasingly targeting cyber space to commit their illegal designs.

2. CYBERCRIME

Cyber-crime is a crime involving, using or relating to computers especially the internet. Crimes involving use of information technology or usage of electronic means in furtherance of crime are covered under the scope of Cyber-crime. The ambit of the term includes all kinds of objectionable or unlawful activities, misuse or abuse taking place in cyber world, through or against the computer, internet, and telecommunication networks run with computer system or technology. The scope of Cyber-crime is bound to increases in view of the ever increasing technological advancement in the area.

3. DIFFERENT TYPES OF CYBERCRIMES

Cyber-crimes are new generation crimes where the achievements of information technology are misused for criminal activities. Such crimes may be committed against the governments, individuals, and institutions. Generally most of the

ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 4, Issue 4, pp: (599-607), Month: October - December 2016, Available at: www.researchpublish.com

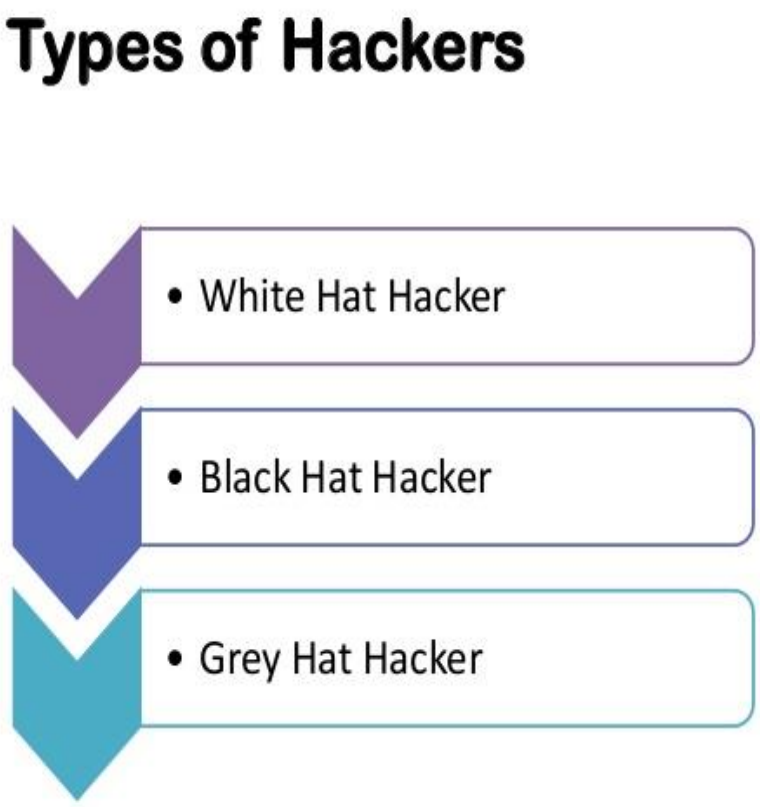
Cyber-crimes are adversely affect individuals, and society at large. The common types of Cyber-crimes are discussed under the following heads:

a) Hacking

Hacking means unauthorized access to another computer system. It is the most popular and commonly known Cyber-crime. Hackers will break into networks and computers system for multiple purposes like data theft, fraud, destruction of data, causing damage to computer system for mere pleasure or personal satisfaction.

Hacking is the basic act of the criminals who later on tread on to the other computer related crimes and frauds thus making it easier for law enforcement authorities to grill them down under other existing laws too. Latest development in this field is hacking of Wi-Fi environment. But the Information Technology Act does not use the term hacking but refers to the same act as unauthorized access to the computer resource.

There are three classes of hackers-white hat hackers, black hat hackers, and grey hat hackers.



DIFFERENT TYPES OF HACKERS:

White Hat Hackers

White Hackers use their hacking skills for good reasons and do no harm to the computer system. So they are referred as ethical hackers.

Black Hat Hackers

A black hat hacker is a person who gains unauthorized access to a computer system with a malicious intention. The black hat hackers use their computer knowledge for private gain. They cause damage to the system after intrusion. They may steal, modify or erase data or insert viruses or women are which damages the system.

ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 4, Issue 4, pp: (599-607), Month: October - December 2016, Available at: www.researchpublish.com

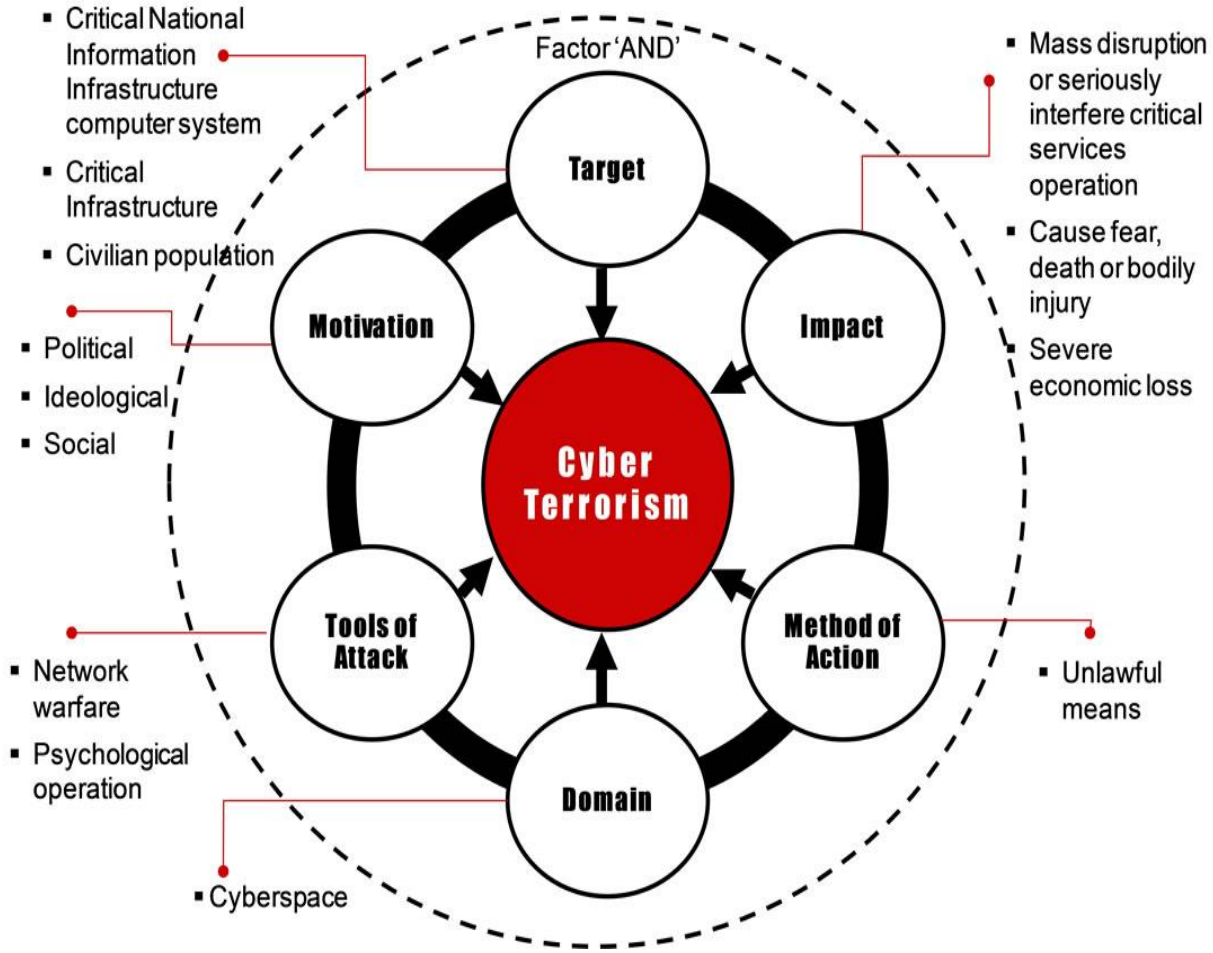
Grey Hat Hackers

A Grey Hat Hackers is a skilled hacker who sometimes acts legally, sometimes in good will and sometimes not. They are hybrids between white hat and black hat hackers. They usually do not hack for personal gain nor have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits.

b) Cyber Terrorism

Cyber terrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threads of attacks against computers, networks and the information stored therein that are carried out to intermediates or coerce a country's government or citizens in furtherance of political or social objectives. Serial attacks against crucial infrastructures could count as acts of cyber terrorism. The cyber terrorism attacks and threats includes interfering and disrupting information and transportation systems, emergency services and government services, communication networks, infrastructure systems, banking and fiancé system.

URE

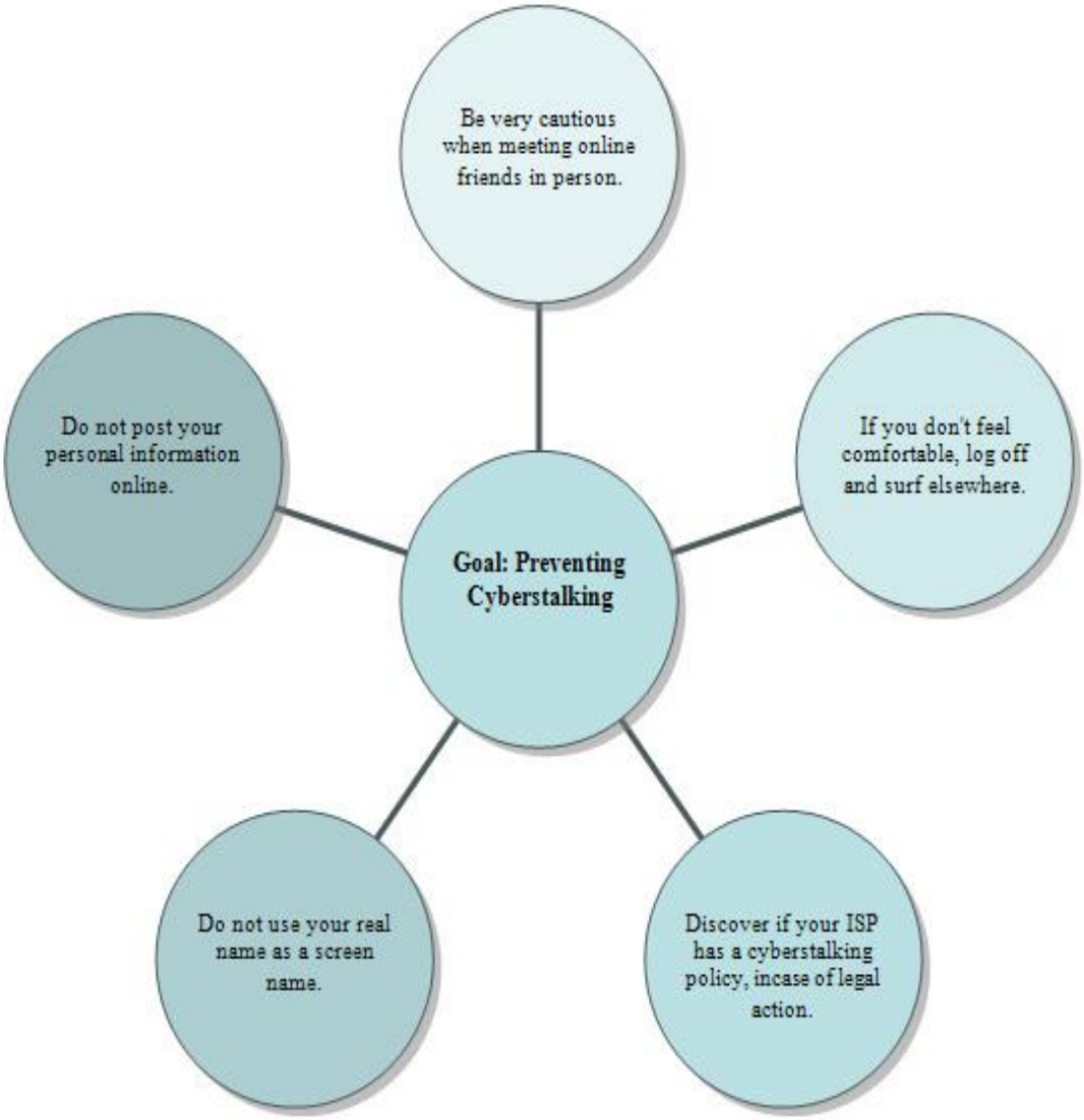


FACTORS OF CYBER TERRORISM:

c) Cyber Stalking

These crimes involve the use of internet to harass someone. The behavior includes false accusation, threats and harassment of as victim through e-Mil. Chat message or web pages. It is a willful conduct that actually causes a victim to feel terrorized, frightened, intimidated or molested. Normally majority of cyber stalkers are men and the majority of victims are women. Since the Information Technology Act, 2000 did not contain any thing relating to cyber staking, the cyber stalkers were booked under Session 509 of the IPC. After the 2008 Amendment to the information Technology Act the cases involving cyber stalking can be charged under section 66-A of the Act and the offender is publishable with imprisonment up to three years and with fine.

ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 4, Issue 4, pp: (599-607), Month: October - December 2016, Available at: www.researchpublish.com



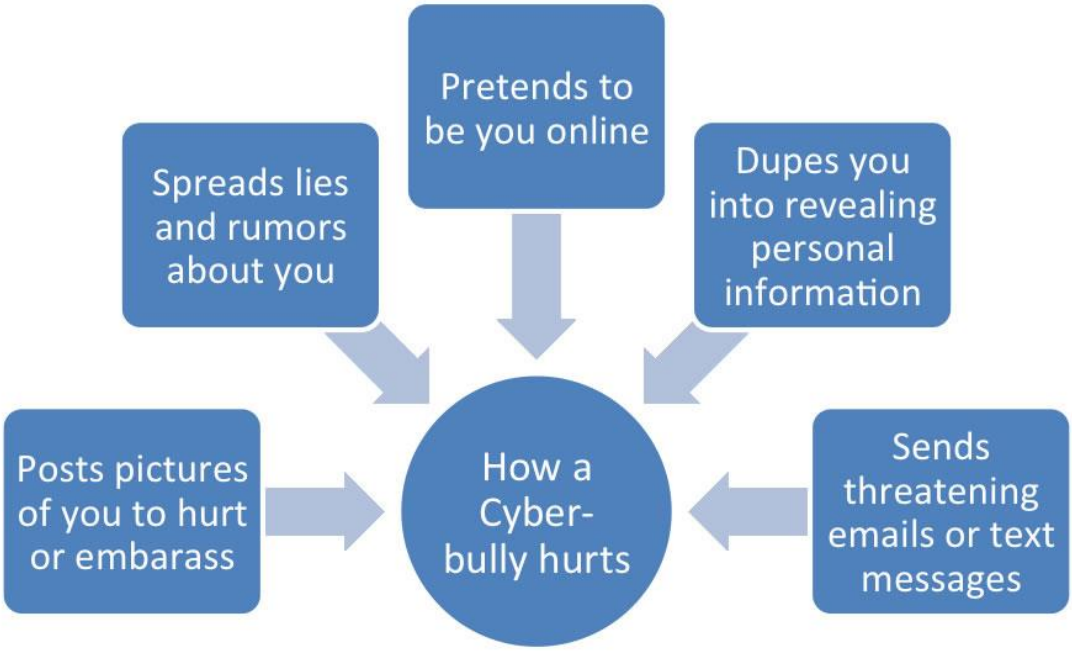
GOAL PREVENTING CYBER STALKING:

In order to prevent cyber stalking the netizens should avoid disclosing any information pertaining to one while chatting. Girls should avoid sending any photographs online participatory to strangers and chat friends as there has been incidence of misuse of the photograph for morphing so as the reduce the chance of netizens becoming victims of Cybercrimes. When children's are involved in cyber stalking it is called cyber bullying.

d) Cyber bullying.

Cyber bullying occurs when children including teenagers are tormented threatened, harassed, humiliated, embraced or otherwise targeted by other children using the internet, interactive and digital technologies or mobile phones. It has to have a minor on both sides or at least should have been instigated by a minor against another minor. The methods used are limited only by child's imagination and access to technology. Cyber bullying is usually not a onetime communication unless it voices death threats or credible threats of serious bodily harm. Cyber bullying may arise to the level of a cyber harassment charge, or if the child is young enough it may result in the charge of juvenile delinquency. In order to safeguard children from cyber bullying parents should be more involved in their children's online activities, the parents should also be aware of major changes in a child's behavior.

ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 4, Issue 4, pp: (599-607), Month: October - December 2016, Available at: www.researchpublish.com



HOW A CYBER BULLY HURTS:

e) Cyber pornography

Cyber pornography refers to stimulating sexual or other erotic activities over the internet. With the increasing use of internet, cyber pornography is widespread. Many websites exhibit pornographic pictures, photos, writing etc….such materials can be produced quickly and cheaply through morphing or through sexual exploitation woman and children. Teenagers are often sexually exploited by their so called lovers and photos taken without their knowledge are published through internet. Such instances are not rare in Kerala also where students and even professionals have been arrested for displaying nude photos of lady students through internet. Children are also exploited by pedophiles using internet. They send photos of illegal child pornography to targeted children so as to attract children to such funs. Later they are sexually exploited for gains. It is reported that in several school in the Kerala numerous girls aged between five and fifteen are prey to sexual abuses. Parents feel that it is increasingly difficult to bring up children's with the traditional value system.

f) Child pornography

Adult pornography is not illegal in many countries but Child pornography is strictly illegal in most nations. Indecent publishing or transmitting information which is obscene in electronic forms are a serious crimes punishable under sections 67 of the Information Technology Act with imprisonment up to 3 years and fine up to 5 lakh rupees for first convictions and with imprisonment up to 10 lakhs rupees for second or subsequent convictions. Publication and transmission of matter containing sexually explicit acts or conduct is to be punished with imprisonment up to five years and fine up to ten lakh rupees and for second or subsequent conviction with imprisonment for a term up to seven years and fine up to ten lakh rupees, the same punishment is prescribed for child pornography.

g) E- mail spoofing

E-mail is the short form for 'electronic mail'. The electronic mail system over the internet can carry messages, letters, pictures, sounds, or anything that can be created and stored in a computer. Data can be send as electronic mail to any other computer connected to the internet, e-mail spoofing is a technique commonly used to hide the origin of an e mail message. The result is that, although the e-mail appears to have come from a particular address it comes actually from other sources.

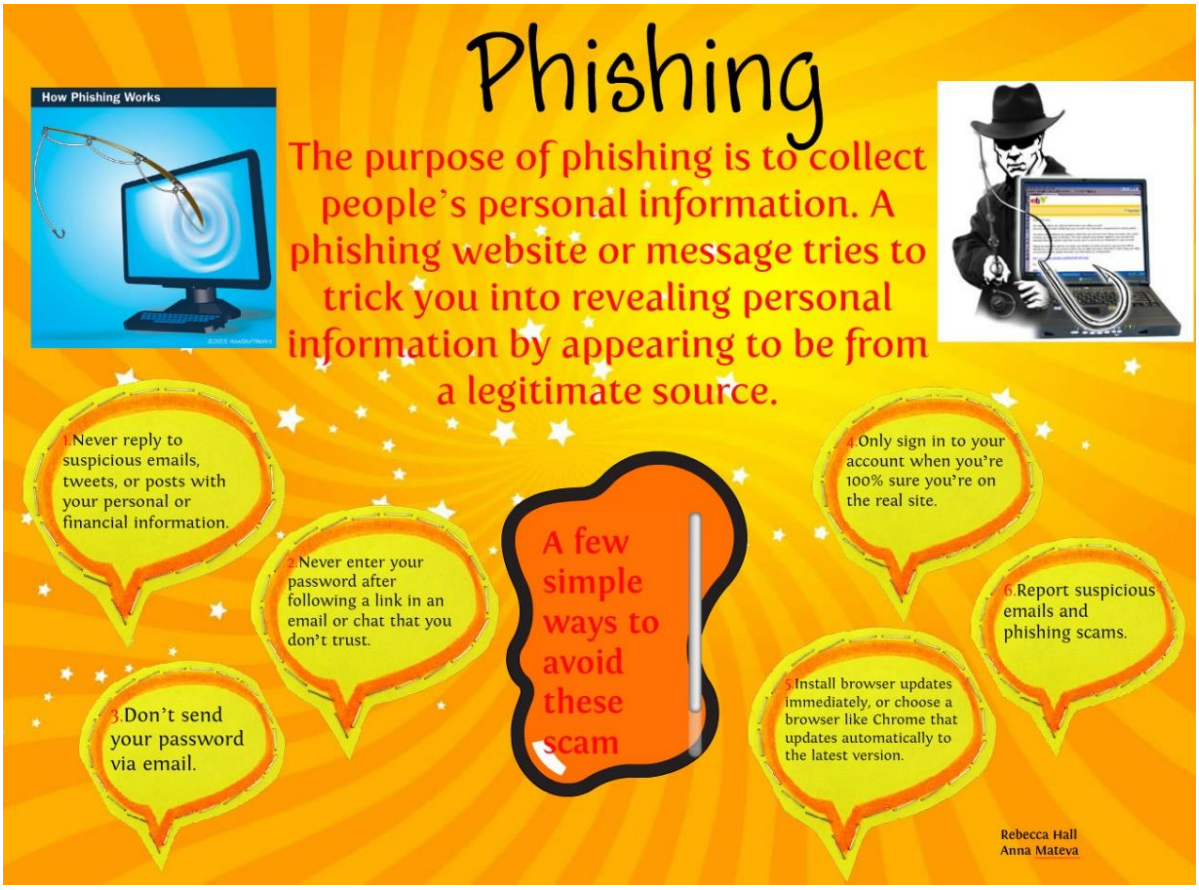
In India the present practice is to charge the offender with forgery under Section 463 of Indian Penal Code for making for electronic records. The punishment is imprisonment of either descriptions for a term which may extend to seven years and fine.

ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 4, Issue 4, pp: (599-607), Month: October - December 2016, Available at: www.researchpublish.com

h) Phishing

It proceeds through the mass distribution of emails that purport to originate from Banks, credit card companies and e-sellers. These mails request for providing personal and other details in order to update their account. The fraudsters thus gain access to the password and other security and authentication information of users, which can then be used to hack bank accounts or steal through credit cards.

According to the Anti-Phishing Working Group (APWG), there were over 2500 such sites reported on the internet in January 2005 alone, a 100% increase in the number in Comparison to previous year (APWG, 2005) Internet offers valuable opportunity to fraudsters to disguise themselves and their identities. These fraudsters also change personal attributes such as age, gender, ethnic group, country of residence and so on. Even though the fraud is detected, identifying the culprit is very difficult Victims of online frauds may be reluctant to report their victimization due to the following reasons. Relatively small amount of money involved does not make pursuing the matter worthwhile, embarrassment in reporting a fraud, ignorance about reporting the offence to the concerned authority, likelihood that no results will ensue as the fraudsters are located in another country.



A literature review is a body of text that aims to review the critical points of current knowledge including substantive findings as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and as such, do not report any new or original experimental work. No study can be undertaken without reviewing and analysing the literature available related to the field of study. Review of Literature is an important component of research by which multifaceted understanding of the phenomenon becomes the part of researcher's cognitive personality. Review of literature on Cybercrime and Social Networking Sites is to find out what research has already been undertaken in the area of Cybercrime and Social Networking Sites, what type of the critical explanations have been given about this new technological crime which is spreading very fast all over the globe, what have been the causes behind occurrence of Online crime and what effect it reflects on Indian society. Besides all this, it is also worthwhile to find out what laws and legislations are present to deal with Cybercrime and issues related to Social media. As the subject of Cybercrime and social networking sites is new in the field of Sociology and Criminology, there is a paucity of literature in this area. Not only this, the available literature has many limitations as the area of Cybercrime and Social Networking is wide and

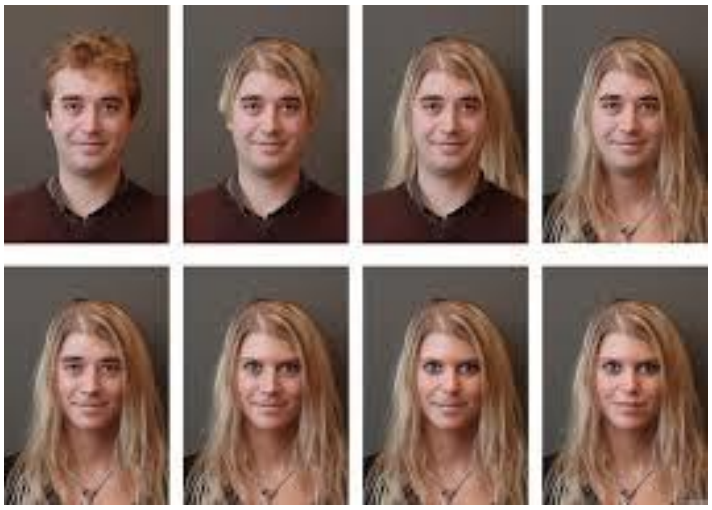
dynamic .Many prominent classical sociologists have contributed towards the social thought on social order, effects of science and technology and crime in society. It is worthwhile to note their viewpoints before reviewing the current literature on technology and crime.

i) Morphing

Morphing is editing the original picture by unauthorised user or fake identity.

It was identified that female's pictures are downloaded by fake users and again Re-posted/uploaded on different websites by creating fake profiles aft editing it. This amounts to violation of I.T.Act,2000 and article sec.43&66of the side Act. The violator can also be booked under IPC also.

The change smoothly from one image to another by small gradual steps using computer animation techniques. Morphing is a special effect in motion pictures and animations that changes one image or shape into another through technological means or as part of a fantasy or surreal sequence



Cyber Theft

Cyber Theft is a way of using a computer and Internet to steal money or in formation. This is also the most popular Cybercrime because the ability to steal from a distance reduces the risk of detection. Cyber Theft includes

j) Cyber Embezzlement

Online embezzlement means misuse or alteration of data by an employee of a company who has legitimate access to the company's computerized system and network. Example an employee misusing the company's computerized payroll system in such a way that he is paid extra. Unlawful Appropriation wherein an individual gains access from outside the organization to transfer funds and modify documents in such a manner that it gives him legitimate right to property he doesn't own. Unlawful appropriation differs from embezzlement as the offender is not interested with the valuables but gains access and transfers funds or modifies some information

k) Corporate Espionage

Corporate Espionage- In this crime, an individual from inside/outside the company uses the network and steals marketing strategies, trade secrets, financial data, client lists etc. in order to gain a competitive advantage. In corporate or industrial espionage, the person uses the company's network to steal trade secrets, financial data, confidential client lists, marketing strategies or information to gain a competitive edge

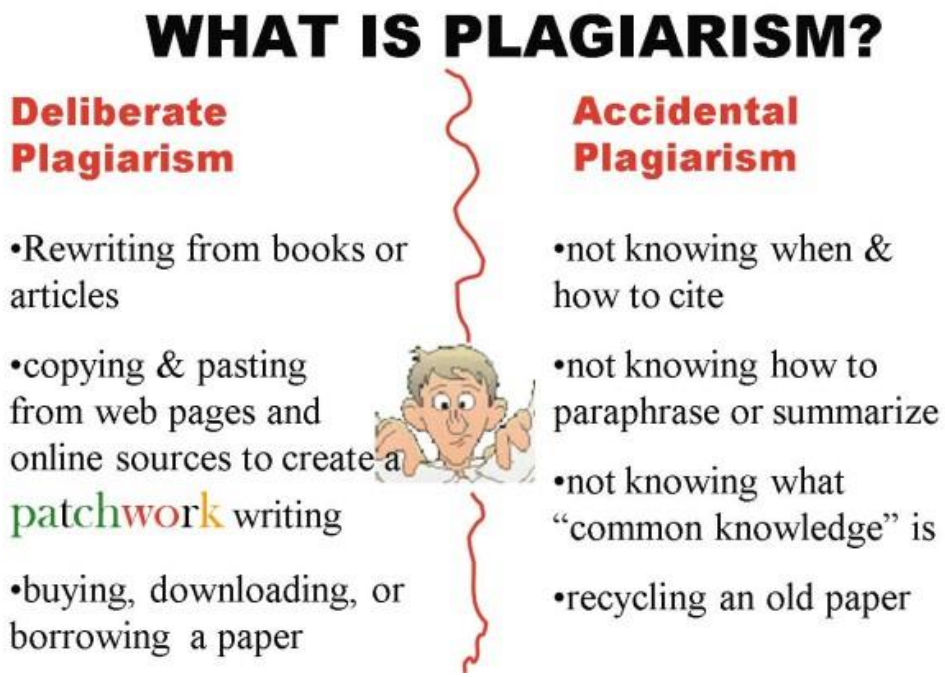
l) Plagiarism

Plagiarism is to steal someone else's original writing and call its own. This form of crime is increasing everywhere as more and more people have access to computers and internet.

Piracyis an unauthorized copying of copyrighted software, video, music, books, etc. which causes loss of revenue to the owner. Cyber piracy is the appropriation of new forms of intellectual property ,in which the computer programme,

expressed in the form of a digital code, generates through a computer system virtual products' such as images, music, office aids or interactive experiences. When cyberspace and intellectual property laws interact they become a powerful force, especially in present day society where economic profit is quite important.

Identity Theft- In this victim's personal information is stolen by the criminal to commit financial frauds.



m) Cyber Fraud

Cyber Fraud Another form of cybercrime which has a firm grip on society is cyber fraud and scams online. But, the problem with this is the lack of systematic and official data. Internet Crime Complain Centre (ICCC)16 is the only source available whose primary role is to receive public reports of cybercrime and refer them to the relevant criminal justice agencies fraction. Hani Duruy, an eBay spokesperson in USA, claims that frauds account for only 0.01% of transactions under taken using the site yet this would amount to 3000 frauds per day, given that more than 30 million actions taking place on eBay daily Cha (2005)17. The fact is that growing number of internet auction sites provide thieves a global market

Through which they sell stolen items to unsuspecting customers. For example, a group of motorcycle thieves in Delhi and Punjab, who is mantled various bikes and sold them online as spare parts for Rs one lakh.Another form of reported fraud is non-delivery of items for which he victims have already paid. It can also include product in authenticity and misrepresentation of the condition of the item. In cases of shill hiding, the seller places false bids by either using multiple fake identities or aliases to place bids on their own items or by arranging for associates to place bids for the items with no intention of actually purchasing them. There after it becomes impossible for the legitimate bidders to detect whether or not others are genuine buyers or shills. In recent years Phishing and spoofing frauds have increased.

4. CONCLUSION

The Study observes use of computers and the change in technology due to new advancements. This Study also cautions the security of internet users and relates this to emergence of Cybercrime. Cyber pornography which is very much rampant, the author also develops a contextual framework on the flow of information on a global level .This Studies mentioned different types of cyber crime, discusses hacking as based on technical virtuosity. The advent of computer networking and the popularity of the internet have also given rise to excessive hacking. Not only this, Privacy is at stack because of widespread online transactions. Mostly people don't know about Cybercrime and Cyber laws. So today's need to aware the society about different types of Cybercrimes and Cyber laws.

REFERENCES

[1] Brenner, W.Susan(2010), *Cybercrime: Criminal threats from cyber space*. Green wood Publishing group, Westport.

[2] Cross, Michael and Shinder, Littlejohn Debra (2008).*Scene of the Cyber crime*, Syngress Publishing Inc, USA.

[3] Flemming, P. and Stohl, M. (2000), Myths and Realities of Cyber terrorism, *International Conference on Countering Terrorism through Enhanced International Cooperation*, 22-24Sept. 2000, Italy.

[4] Furnell, Steven (2002), *Cybercrime: Vandalizing the information Society*, Addison-Wesley, Boston.

[5] Higgins, George (2010), *Cybercrime: An Introduction to an Emerging Phenomenon*, McGraw Hill Publishing, New York.

[6] Holt, Thomas J (2011), *Crime Online: Correlates Causes and Contexts*. Durham, Caroline Academic Press, USA. India is now world's third largest Internet user after U.S. *and* China; The Hindu; Aug 24,2013

[7] Jaishankar, K.(2001). *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*. CRC Press: Taylor and Francis Group.

[8] Kerala State Legal Service Authority, Cochin (2013) *Lessons in Law.* Cochin Printed Pvt. Ltd. Eloor.

[9] Skinner W.F. and Fream A.M. (1927), A Social Learning theory analysis of computer Crime Among College Students, *Journal of Research in Crime and Delilnquency*,Vol 34, 495-518. Sutherland, Edwin H. (1924), *Principles of Criminology*, University of Chicago Press, Chicago.

[10] Wall, David S (2001*), Crime and the Internet*, Routledge, London.

[11] http://cybercrime.planetindia.net/intro.htm 20/11/201

[12] http://www.cyberlawsindia.net/black-hatml.7/4/2015

[13] http://www.stopcyberbulling.org/what-is-cyberbulling-exactly.html.21/3/2015

[14] http://www.cyberkeralam.in8888/common/cybersecurity.jsp.2/11/2014

[15] http://www.interpol.int/public/technologycrime/crimeprev/itsecurity.asp#21/4/2015