ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/2492
DOI URL: http://dx.doi.org/10.21474/IJAR01/2492

RESEARCH ARTICLE

A SOCIOLOGICAL ANALYSIS OF CYBER CRIME SECURITY AWARENESS AMONG TEENAGERS.

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

Manuscript Info

Manuscript History

Received: 23 October 2016
Final Accepted: 21 November 2016
Published: December 2016

Key words:-
Education, Internet, Cybercrime, Disadvantages, Modern, Students.

Abstract

The advent of e-technology has brought variety of opportunities and some of these, not surprisingly, are of a criminal nature. The Cyberspace created by computer technology provides a medium for doing many things in efficient manner. The automations use of machine replacing human hands provided great opportunities and options. The connected computer machines have created a different world called Cyber world or cyber space. It is a different world altogether, quite different from our real world! Due to special nature of this Cyberspace the cyber criminals get maximum opportunity to commit crime. Cybercrimes are committed by using mobile phones, computers, scanners, digital cameras and other electronics devices.

In the modern educational field rapid changes are happening in a vast country like India. Enormous developmental work is now being done in the field of education so as to enable students to get a better vision of life in other parts of the world and scientific development around the globe. The "Internet" in India is growing rapidly; it has given rise to new opportunities in every field: - be it entertainment, business or education. Internet also has its own disadvantages; one of the major disadvantages is "Cyber-crime" i.e, illegal activity committed on the internet.

Introduction:-

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

Corresponding Author:- Dr. Grace Varghese.
Address:- Pullannivelical House Mylapra Town P.O Pathanamthitta Dist Kerala, India.

decades, a huge gap between Cyber technology and Cyber criminality has happened without any hope of bridging the gap.

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. Majority of the victims of Cybercrimes are children of adolescent age.

Recently in Kerala an incident was reported in which three girl students of which one committed suicide and the other two are surviving remind victims of Cybercrimes. The nude pictures of these girls were circulated on the internet by their own boyfriends who were later arrested by police.(Mathrubhumi, 2014)

In another incident in Kerala, teachers were blackmailed by one of their students by morphing the body of another person and uploading their photos in Face book. This is how students use the internet illegally and commit Cybercrime. (Malayala Manoramma, 2014)

Nowadays people have started to think that hacking is only hijacking Facebook accounts. A relevant example is of the official website of the Pakistan People's Party (PPP) that was hacked earlier this month by a 16year old Indian boy, apparently due to Bilawal Bhutto's provocative speech on Kashmir.(Indian Express 2014)

Education Awareness about Cyber Crime:-

The educational curriculum of these courses on computer technology hardly contains the awareness about Cybercrime. Students are not aware of the consequences of Cybercrime and its punishment. That is a reason why they fall in to such traps. So the Parliament of India enacted the Information technology Act in 2000, framing a uniform regulation in the field of electronics governance, e-commerce and Information technology. Under the act certain violations are treated as serious crimes and offenders are liable to penal actions. In this context it is important that awareness is spread on the existing problem and laws related to it.

The Government has an important role to play in cyber security assurance in the form of long-term strategies. A cyber security strategy has been outlined by the Department of Information Technology, Government of India, to address the strategic objectives for securing country's cyber space and is being implemented through the following major initiatives. It focuses on creation, establishment and operation of cyber security assurance framework aimed at assisting government, critical infrastructure organizations and other key users of nation's economy. Protection of Critical Information Infrastructure, augmentation of facilities at Computer Emergency Response Team (CERT), creation of sectoral CERTs, enhancing global co-operation among security agencies, promoting national awareness programs and training on cyber security, security research and development are some of the strategies adopted by the Government. It also focuses on creation of national cyber alert system for rapid identification and response to security incidents and information exchange to reduce the risk of cyber threat and resultant effects.

There is no serious provision for creating awareness and putting such initiatives in place in the Act. The government or the investigating agencies like the Police department (whose job has been made comparatively easier and focused, thanks to the passing of the IT Act), have taken any serious steps to create public awareness about the provisions contained in these legislations, which is absolutely essential considering the fact that this is a new area and technology has to be learnt by all the stake-holders like the judicial officers, legal professionals, litigant public and the public or users at large. Especially, provisions like scope for adjudication process are never known to many including those in the investigating agencies.

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws are a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Cyber law Awareness program will cover:-

1. The basics of Internet Security.
2. Basic information on Indian Cyber Law.
3. Impact of technology aided crime.
4. Indian IT Act on covering the legal aspects of Online Activities
5. Types of Internet policies required for an Organization.

Information is a critical asset. Therefore, it must be protected from unauthorized modification, destruction and disclosure. This brochure describes information security concepts and defines steps required to properly safeguard information. It is the responsibility of everyone employee and home user to become familiar with good security principles and to follow the information protection tips.
Therefore the investigator, in the case of this study, tries to focus on the creation of a module that will spread awareness on the Cybercrime and the laws that are related to the crime.

Need and significance of the study:-

It is important that initiatives are taken in the education sector itself for understanding the issues involved in Cybercrime. One important step forward in this direction is to spread awareness among adolescent students against the crime and encouraging them to utilize the positive side of the internet. Every person in the world is dependent on Cyberspace in one way or another, directly or indirectly. Cyberspace is open to participation by all. And interactions between students, scholars and teachers across continents are made possible by the internet. If internet is used wisely it can help in minimizing the gap between the 'haves' and 'have-nots' of the world.

This study aims to test the effectiveness of an instructional module that is meant to be distributed among students with the aim to spread awareness on Cyber crime and the laws against it. It is the need of the hour that such a study is conducted in schools as newspaper reports suggest that adolescent people, especially those who go to higher secondary school fall prey to such activities the modern thief can steal more with a computer than with a gun. Tomorrow's terrorists may be able to do more damage with a keyboard than with a bomb. Information and technology are all encompassing. They have brought transformation from paper to paperless world. Internet has dramatically changed the way we think, the way we live, the way we govern, the way we do commerce and the way we perceive ourselves. Information Technology encompasses all walks of life, all over the world.

Cyberspace is full of opportunities. However like in real life, good and bad practices exist in this sphere too. Moral, civil and criminal wrongs are committed in internet. It has now given a new way to express criminal tendencies. It has become a space for power play between nations. Instead of utilizing the good side of the internet, new ways to intimidate and threaten the perceived enemies are created. Fighting bad practices spread through internet is found to be a challenge by educational institutions all over the world.

It is in the interest of the educational sector all over the world that innovative and enabling legal infrastructure in tune with the times is put in place. Students who are gullible due to their tender age and inexperience are particularly vulnerable as far as criminal tendencies in internet are concerned. New legal tools developed against exploitation of vulnerable groups in cybercrime should focus on students. It is a fact that cybercrime is here to stay and it has to be treated as a 'necessary evil'. As far as education sector is concerned, welfare of the students should be compelling enough for us to move forward regardless of the problems and we should move ahead by creating legal tools for utilizing the positive sides of internet while minimizing the harm.

We are in the period of 'Information Explosion'. The electronic and digital media have completely changed the Indian social scenario. All types of information reach home easily. This has not only changed the psychology of people but also changed their behaviour and life style. Even though information explosion has affected all sections of society, it is the youth and adolescents who are most influenced by the technological spurt. Information Revolution has given impetus to the process of Globalisation. Due to information explosion all types of control on the flow of information are impossible.

Newspapers are read online and mobile use is expanding. Internet is the heart of the Information revolution. Youth and adolescents are more diligent Cyberspace consumers. Internet occupies a central position in present day mass media society and internet activities seem to be a natural element in leisure. Internet use today serves not only as a mirror of society but also as an instrument of social change .The use of Cyberspace is now more and more

individualized. Furthermore, in the contemporary era the geographical distances play a vague role. Social relations are lifted from the physical context. This is all because of technological development. In network society, we organise our lives around mass and social networking society. It seems natural for us to see the media as anchored in the private spheres. A radical change is evident in the norms and lifestyle of adolescents in modern India. The impact of westernization and globalization has made young generation techno survey and leisure oriented.

One of the most noticeable changes is the adolescent's preoccupation with electronic gadgets such as mobiles, I pads, laptops or in other words their heightened "technical consciousness". The past ten years have witnessed the emergence of a new phenomenon i.e. Social Networking sites. Networking is as old as Human Society. Human beings have always sought to live in a social environment. However, now networking has shifted towards Internet to significant extent. This is an activity in which millions of internet users are involved both in their leisure time and at work. However, there has been very little research on the impact of these sites on adolescents in the Indian context. The world of Internet continues to expand as does the research about its use by adolescents. Thus, with this background an attempt is made in this study to analyse the impact of networking on adolescents and their life style .An attempt has been made to find out their activities on social networking sites and whether they provide a new venue for adolescents to behave in a deviant manner.

The study also attempts to identify why adolescents are more likely to involve in deviant behaviour through social networking sites. For this individual attributes such as age, sex, education and parent's income are used to construct a predictive model. Further, this study also analyses various types of Cybercrimes on internet sites in which adolescents are either victims or perpetrators. For an understanding of the ideas, values, attitudes and aspirations of the adolescents, certain sociological variables are taken into consideration to know how they influence the behaviour of the adolescents. The variables such as age, sex composition, family income, and school background provide the profile of adolescents. Adolescents form an important group in the use of networking sites.

The study covers the adolescents ranging from 13 years to 17 years. Information technology has spread throughout the world. The computer is used in each and every sector wherein Cyberspace provides equal opportunities to all for economic growth and human development. As the user of Cyberspace grows increasingly diverse and the range of online interaction expands, there is expansion in the Cybercrimes i.e. breach of online contracts, perpetration of online torts and crimes etc. Due to these consequences there was need to adopt a strict law by the Cyber space authority to regulate criminal activities relating to Cyberspace and to provide better administration of justice to victims of Cybercrime. In the modern cyber technology world, it is very much necessary to regulate Cybercrimes and most importantly cyber law should be made stricter in the case of Cyber terrorism and hackers.

Mostly people don't know about Cybercrime and Cyber laws. So today's need to aware the society about Cybercrimes and Cyber laws. The present studies the investigator try to give the awareness programme about Cybercrime and its law.

Cyber Law:-
Cyber law is the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, and hardware information systems. (National Research Council,2013)

In the present study cyber law is the area of law that deals with the internet's relationship to technological and electronic element, including computers, software, and information systems.

Module:-
Module explores some key educational concepts and applies them to clinical teaching and learning situation (www, webcrawler.com 2014)

A unit of education or instruction with a relatively low student to teacher ratio, in which a single topic or a small section of a broad topic is studied for a given period of time.

Security Awareness:-
Awareness as the quality on state of being aware consciousness aware is defined as informed, cognizant, conscious, and sensible.

In this study the purpose of cyber security awareness presentation is simply to focus attention on cyber security. Awareness presentation is intended to allow individuals to recognize information technology security concerns and respond.

Investigator go review seriously so many literature regarding the chapter Cybercrime and related concepts, investigator didn't identify any study relating the awareness of an testing of an instruction that develop the awareness among secondary school students, that is motivating her to take up study on the area of Cybercrime especially among the school children more one last of experience a school teacher she handled so many issues relating the Cybercrime among the children that also learn to develop an instructional module for developing information security awareness.

In the present study the module deals with basic awareness of various Cyber related Crimes,

1. Consists of information regarding various Cyber gadgets, sources of Cyber manipulation, creation of various fake information.
2. Laws and punishments
3. Educating the students for the purposeful use of Cyber gadget.
4. Spreading awareness on different legal acts that may apply in the case of Cybercrimes.

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.

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

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.

Different types of cybercrimes, it act and its punishments:-

Cybercrimes	IT Act	Punishments
Impersonation (fake) profiles, in community networks, fake e-mail Ids etc…)	66 D of IT Act 419 IPC	3 years and fine up to 1 Lakh
Cheating (lottery scam using e mails and SMS, fake websites, mail asking financial helps etc…)	66 A, 66A (b) (c),66 D 420 IPC	3 Years and fine
Software theft (using the source code of software and creating another).	66 A r/w 43 (j)	3 years or fine up to 5 lakhs or both
Morphing (editing the photo with nude photo and publishing)	66 C r/w 43 (i),66 A(b),509 IPC	3 years or fine up to five lakh or both
Cyber terrorism (crimes against the Nations by means of computer /mobile/internet etc.	66 F of IT Act	Up to life imprisonment.
Spoofing (hiding identity and using others identity)	66D of IT Act	3 years and fine up to 1 lakh
Website Hacking	66C r/w 43(a)	3 years or fine up to 5 lakh or both

Email Hacking (methods are phishing, new website. Account registration) etc	66 E r/ w 43(a)	3 years or fine up to 5 lakh or both
Pornography (makes people especially children leading psychic states that cause rape, child molestation, sex, exhibitionism, sexual violence etc…)	67,and 67A of IT Act	5(7) years and fine up to 10 lakh
Child pornography(hidden in pornographic sites)	67 B of IT Act	5(7) years and fine up to
Credit / ATM card Frauds (using scanner and camera)	420 IPC 66 D 0F IT ACT	3 years and fine up to 1 lakh
Taking video /photo of women or spreading it	119 (b) of KP ACT	3 years or RS.10,000 or both

Conclusion:-

The present study was concluded in such a way that the Module on Cyber laws is more effective, The investigator should develop the module about different types of Cybercrimes, and its consequences. It helps to develop the curiosity among the students to know about the crimes in our locality. Such controls include personal security and incident handling measures to prevent fraud and security breaches.

The study observes that majority of the adolescents are online daily for along period of time due to which their studies are affected negatively resulting in poor academic grades. It is also observed that students who use social networking sites on a regular basis tend to have negative effect on health such as stomach aches, poor sleep patterns, eye strain, anxiety and depression. The study reflected that the adolescence are having on online addiction in which an individual forgets his/her real life and finds solace in virtual life. This trend makes a person avoid his real life problems and indulge in cyber space. This is having adverse effect to the personality of adolescents who have framed their dual identity one in the real world and another in the virtual world.

The present study proves that the Module on Cyber law is highly effective for the development of cybercrime awareness among higher secondary school students.
The role of an educator is not merely teaching students theories and facts.To enhance the learning experience of every students, the educator has to cater to many different learning styles and capacities.

The présent study provide sastrong base for analyzing the technological implications on adolescent behaviour in the domain of society. In this study is to shed light on the role of social networking sites on adolescent internet users and their effects on social, physical and psychological aspects of adolescents. The present studies shows that adolescent users belonging to 16-17 years of age group have easy access to internet in comparison with other age groups and they easily convince their parents for the same.

Here the studies have suggested that the unique features of Cyber law for developing information security awareness is a powerful technique device. This technique once learnt, can be utilized throughout an individual's academic life and modified to be used in working life as well. As an educator, it is imperative that all potentially beneficial teaching and learning techniques are explored and passed on to students in order to cultivate realization that the learning process is an infinite continuum.

References:-

1. **Akers, Ronald L**. (1998), *Social Learning and Social Structure: A General Theory of Crime and Deviance*, North Eastern University Press, Boston.
2. **Arquilla, John and Ronfeldt, David and Monice, Santa** (2001).*Networks and Netwars: The future of Terror, Crime and Militancy*. The University of Michigan press, USA
3. **Baudrillard, J.** (1984), *Simulations.* Semiotext (e), New York
4. **Bill Gates** (1995). *The Road Ahead, Viking*, New York.
5. **Carey, James W.** (1993). Everything that rises must diverge: Notes on Communication, Technology & the Symbolic Construction of the social, *Beyond Agendas*, 171-184, Westport, Connecticut, Greenwood.
6. **Das, Biswajet and Sahoo, Jyoti** (2011), *Social Networking Sites. A Critical Analysis of its impact on Personal and Social life. International Journal of Business and Social Science*, **Vol.2** (14)
7. **Higgins, George** (2010), *Cybercrime: An Introduction to an Emerging Phenomenon,* McGraw Hill Publishing, New York.

8. **Jaishankar,K** (2007),Establishing a Theory of Cyber Crime ,Pg 7-9*International Journal of Cyber Criminology* ,Vol 1 Issue 2
9. **Mohan Rama.U and Barkha**(2014*).Cyber Law and Crimes.*Harita Graphics,Hyderabad
10. **Thomas, Douglas and Loader Brian (2000),***Cybercrime Law Enforcement, Security and Surveillance in the Information Age*, Pg 8,Routledge, London.
11. **Young, Kimberly (1998**), Internet Addiction: The Emergence of anew clinical Disorder, *Cyber Psychology and Behavior*, Vol. 1-No.3, Pg. 237-244.

Websites:-

1. http://www.legalserviceindia.com/article/1129-Torts-In-India.html (20/5/2015)
2. http://www.cyberlawsindia.net/black-hatml.7/4/2015
3. http://searchsecurity.techtarget.com/definition/adware.27/5/2015.
4. http:// www.mit.gov.in/content/strategic-approch.20/2/2015.
5. http://www.interpol.int/public/technologycrime/crimeprev/itsecurity.asp#21/4/2015