



A Study on Awareness of Cybercrimes Among Youth

¹Nirav Jadhav, ²Mr. Vimal Makwana

¹MSW Student, ²Assistant Professor

^{1,2}Faculty of Social Work, Parul University, Limda, Waghodia, Vadodara, Gujarat

Abstract-

People dependence and behaviour towards information security and internet deeply affect the way they intend to use information technology. The increased dependence of people on internet has led to the rise in cybercrime. Problems such as lack of proper training and education, the poor awareness of cybercrime Among Indians have also contributed to the growth in cybercrime. Even the law enforcement has faced huge Problems in tackling cybercrimes due to the high rate of cybercrime. The paper intends to understand the Awareness level of cybercrime among various college youth of Vadodara. The paper also intends to find out the college students' awareness on the types of cybercrimes and the various government schemes. The paper also finds out the various precautions taken by a student while using the internet. A questionnaire survey was conducted among 70 college youth of Vadodara the state of Gujarat to collect the required data.

Keywords: Cyber Crime, Youth, Awareness, impact of cyber crimes

I. Introduction

According to Webopedia, "any criminal act dealing with computers and networks (called hacking)" is considered cybercrime. A variety of illegal digital activities aimed at harming organizations constitute cybercrime. According to Norton Company, the simplest definition of cybercrime is "a crime that has some kind of computer or cyber aspect to it." Norton claims that cybercrime steals an individual's identity every three seconds. Cybercrimes do not take into account borders or barriers to territory. All stakeholders are most concerned.

About making the cyber world safer. As a result, in order to curb cybercrime, each nation will have its own cyber law or Internet law. The Information Technology Act, 2000, was also drafted by the Indian government. This act applies to India as a whole and is meant to make electronic data interchange and other forms of electronic communication transactions legal. The following are, in decreasing order, the top five criminals:

- Loss or Damage to computer resource or utility
- Obscene publication/transmission in electronic form
- Hacking
- Tampering computer source documents
- Breach of confidentiality or privacy

Types of Cybercrimes most prevalence in India:

Using a computer network, such as email, videos, or phones, to afflict a person with fear for their life, the lives of their families, or the safety of those they are responsible for (such as employees or communities) is considered assault by threat.

Child pornography is the creation, distribution, or access to materials that sexually exploit minors using computer networks.

Cyber laundering is the electronic transfer of funds obtained illegally with the intention of concealing their source and, possibly, their destination.

Cyber stalking is the use of computer technology, such as email, phones, text messages, webcams, websites, or videos, to evoke fear and express or imply physical threats.

Premeditated, typically politically motivated acts of violence committed against civilians using or aided by computer technology constitute cyber terrorism. Using a computer to steal is known as cyber theft. This includes the following activities: espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy are all forms of breaking and entering, DNS cache poisoning, embezzlement and illegal appropriation, and embezzlement.

Hardware Hijacking: A serious security flaw in some printers was also recently discovered by Columbia University researchers. When a print job is accepted, many printers automatically connect to the Internet to download the most recent print drivers.

Spam is more than just annoying: Unsolicited mass email is also known as "spam." Spam messages can be used as carriers for computer worms and viruses or to trick people into giving away personal information (known as "phishing").

Script kids: An aspiring hacker, someone who wants to be a hacker or thinks they are one, but doesn't have any real technical knowledge. Most of the time, they can only attack very weakly secured systems.

II. Research Methodology

Main Objective:

The Present research was an endeavour to evaluate awareness of cybercrimes among youth

Sub Objectives:

- To study the awareness of cybercrimes among youth.
- To study the causes of cybercrimes among youth. .
- To study the impact of cybercrimes among youth
- To study the opinions on eradication of cybercrimes

Research Design

Research design is the framework that has been created to seek answers for the research questions. In essence, a research design is a map or blueprint of the study. By design, the present study is descriptive as the study describes the awareness of the youth on cybercrime. A survey research design is one that is concerned with describing the characteristics of a particular individual youth. The focus of this design is placed on describing the events and situations. In addition, the study aims to describe the nature and extent of victimization, and the impact of victimization.

Universe of the Study:

The universe of the study includes youth victims and awareness of cybercrimes. The study is confined to the city of Vadodara. The respondents for the present study were the youth. A total of 71 youth were found elsewhere and the researcher had made several attempts to get responses from neighbours & society. Therefore, the present research work has been conducted with a study population of 71 youth in Vadodara city.

Sample and sampling size:

Sample is the representative of the whole universe. Here, the researcher has used simple random sampling method, and selected 71 respondents.

Primary Data:

Tool for the data collection will through questionnaires.

Secondary data:

Internet, books, previous dissertation, journals.

Limitations of the study:-

The present study is subject to the following limitations.

Even though there are many causes of cybercrimes the present Study cover only awareness, knowledge of awareness of cybercrimes and its causes and impact. Districts areas have been selected on the basis of random sampling methods. Some of the respondent are not even know what cybercrimes is and some have good knowledge in it.

III. Findings

- The majority of the respondents (53.3%) are Female.
- The majority of the respondents (71.8%) are belongs to the age group of 21-25 years.
- The majority of the respondents are Post-Graduate.
- The majority of the respondents are feels that they are pretty much educated about cybercrimes.
- The majority of the respondents are feels that the effort made by school/collage are neither well nor inadequate.

-
- The majority of the respondents are using antivirus software in their PC/Laptop.
 - The majority of the respondent are not feeling safe for being online.
 - The majority of the respondents are feel essential to be safe online.
 - The majority of the respondent are not ever been victim of cybercrimes till now.
 - The majority of the respondents never loses money due to any cybercrimes.
 - The majority of the respondents will prefer to tell police if something bad will happen to them in context of cybercrimes.
 - The majority of the respondents are aware about invasion of privacy in cybercrimes.
 - The majority of the respondents feels that after digitalization cybercrimes cases are increase in India.
 - The majority of people believe that Identity theft, spamming, Hacking, Cyberbullying, Invasion of privacy are some types of cybercrimes.
 - The majority of the respondents are believe that cybercrimes rate is increasing day by day due to use of social media.
 - The majority of respondent believe that cybercrime affect the political growth, economic growth, social growth and structural growth of the country. Hence it effect all over growth of the country.
 - The majority of the respondents are agree that cybercrimes effect society both online & offline.
 - The majority of the respondents are agree that becoming victim of cybercrime have long lasting effect on life.
 - The majority of the respondents are agree that emotional, social security and monetary losses can occurs after becoming victim of cybercrimes.
 - The majority of the respondents believe that laws are helpful in prevention of cybercrimes in India.

IV. References

- <http://www.navi.org/pati/cyberobscentiv.html>.
- <http://www.cyberlaws.net>
- <http://www.cybercash.com>
- <http://www.apiap.org/opinions/legal>
- <http://www.netsafetv-nic.in>