

A STUDY OF THE AWARENESS OF CYBER CRIME AND CYBER LAWS AMONG PEOPLE WITH RESPECT TO MUMBAI REGION

Ankita Awsarmal

Asst. Professor

Laxmichand Golwala College of Commerce & Economics

Abstract

21'st Century has been characterised by technological innovations that have shape the way people interact. In India each and every minute one person become internet users. Its convergence with digitally supported platforms and gadgets, safeguarding the parents as well as students from the cybercrimes is becoming a challenging task. Cybercrime grows quickly with developing newer techniques every day. According to survey of 2021, 70% of people, businesses, corporate affect by Cyber Attack. This study examine that various types of cybercrimes worldwide and there is rapid increment in it day by day. IT Act 2000 law established in INDIA to concrete legal framework, establishment of cybercrime Law enforcement organizations. Cyber Crime used different methods in Modern era. This research paper particularly focuses on the Awareness of Cybercrime and Cyber Laws to highlighting their importance towards the people. The paper suggested a conceptual model explaining how to uphold and implement the awareness programmes among internet users regarding cybercrimes. This Study was done in all over the Mumbai Region where data was collected from 162 people who have experienced some cyber-attacks.

Keywords: *Cyber Crime, Cyber Laws, Computer Crime, Unauthorized, Cyberattacks.*



Aarhat Publication & Aarhat Journals is licensed Based on a work at <http://www.aarhat.com/eiirj/>

Objective:

- ★ To study about the awareness of cybercrime among people.
- ★ To study about different ways through which people can protect themselves by using Cyber Laws.

Introduction:

Cyber Crime:

Cyber Crime referred to as “Electronic Crime”, “Cyber Attack” and “Computer related Crime. There have different classifications and types of Cyber Crime or Cyber Attacks. Cybercrime can be categorized into two types: Type I and Type II depending upon the intensity of the crimes. Type I refers to the cybercrime activities that are technical, for example: Web Hacking. On the other hand Type II refers to human interaction rather than technology for example: spoofing, cyber staking, criminal activities such as identity theft, Credit card fraud, harassment. There are many cases where judgement cannot describe cybercrime, we need to identify it with possible ways. Cyber Crime basic classification shown in below figure 1.

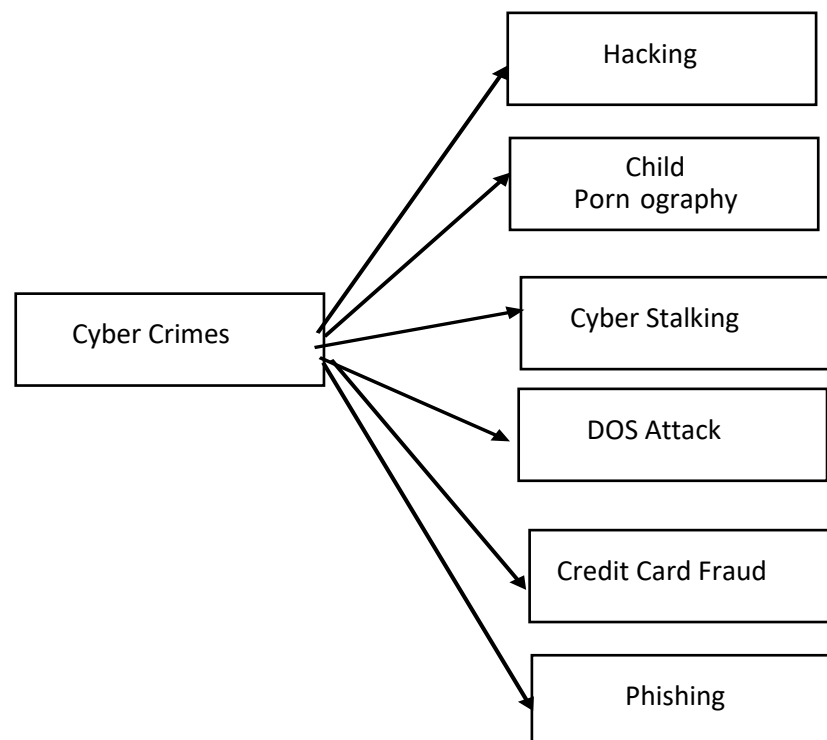


Figure 1: Classifications of Cyber Crime

Cyber Laws:

The evaluation of information technology (IT) has brought about successful communication through the internet and global interaction through Social Media platforms. Cyber laws used



for the digital circulation of information, software, information Security.

The Information Technology Act, 2000 (“IT Act”) established in INDIA to address the computer technology, mobile devices, software, and the internet are medium to identify such crimes. It is used to provide legal recognition to electronic commerce and filing of electronic records with the government. Intersection of many legal many fields including intellectual property and privacy. There are many other Cyber laws established in India

Information Technology

Amendment Act 2008.

Cyber Crime



Review of Literature:

1. Bhanu shahu, Neeraj Shahu, International Conference on Communication System and Network Technologies, 2013: “Identify Uncertainty of Cyber Crime and Cyber laws”. This study was conducted in order to understand effects of Cyber Crime and various types of Cyber Attacks. It highlighted effects and what kind of security measure we have to take to overcome with the cyberattacks. In this paper conduct survey of cybercrime all over the worlds including total Top 20 countries. The most Affected country by cybercrime is United State of America.
2. Mohammad I. Alghamdi, International Journal of Engineering Research & Technology (IJERT), June 2020: “A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide”. In this research paper has study about that cybercrime is fast gaining around in both developed and developing countries. It discovered that conventional laws and policies are currently incapable of mitigating cybercrime cases.

Research Methodology:

In the Cyber Crime different methods are used. These methods uses classification of Cyber



Crime.

1. *Hacking*: An illegal activity in computer and smartphone is known as Hacking.
2. *Child Pornography*: The Internet used by its abuser to reach and abuse children sexually with the worldwide.
3. *Cyber Stalking*: Cyber Stalking defined as repeated acts harassment behavior of the cybercriminal towards the victim by using internet services.
4. *Virus Dissemination*: Malicious Software installed automatically and it's attached itself to the software.
5. *IRC Crime*: Internet Relay Chat (IRC) servers have chat rooms in which people from all over the world can come together and chat with each other.
6. *Credit Card Fraud*: The unauthorized user and illegal use of credit card to access the account and property.
7. *Phishing*: It is the type of attack also called as social engineering attack that attacker steal the user data including login details, credit card numbers. For Example. Google Doc Scam, Pay Pal Scam.

This study uses the qualitative method that intends to collect comparable records on cybercrime and computer crime activities across the world.

The Cyber law in INDIA is the law regarding Information Technology including Computer and Internet.

Importance of Cyber Law:

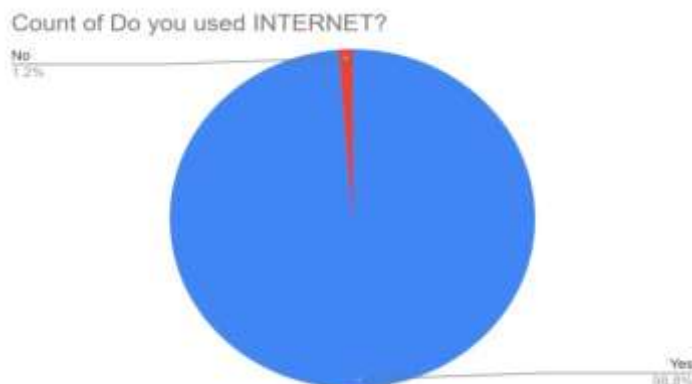
- ★ It covers all transaction over an internet.
- ★ It keeps eyes on all activities over an Internet.
- ★ The major area of Cyber Law include Fraud, Copyright, Defamation, Harassment and Stalking, Freedom of speech, Contract and employment Law.

Data Analysis & Interpretation:

The data collected from people with the help of questionnaire has been analyzed & interpreted. The interpretation of data has been represented in diagrammatic format.

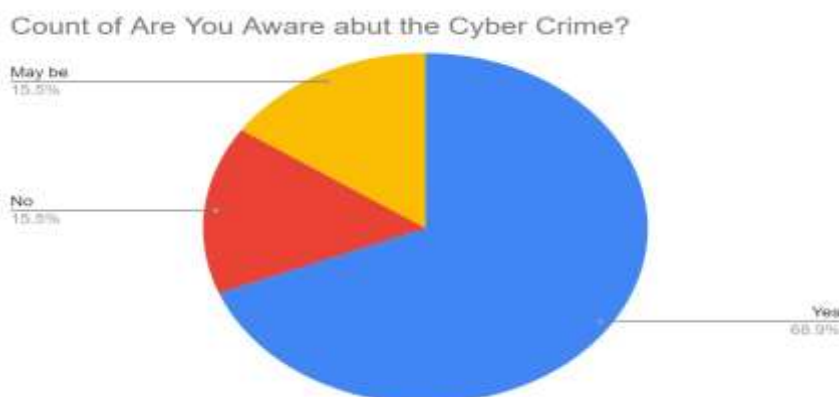


Electronic International Interdisciplinary Research Journal
Volume-XI, Issues-I *Jan - Feb 2022*

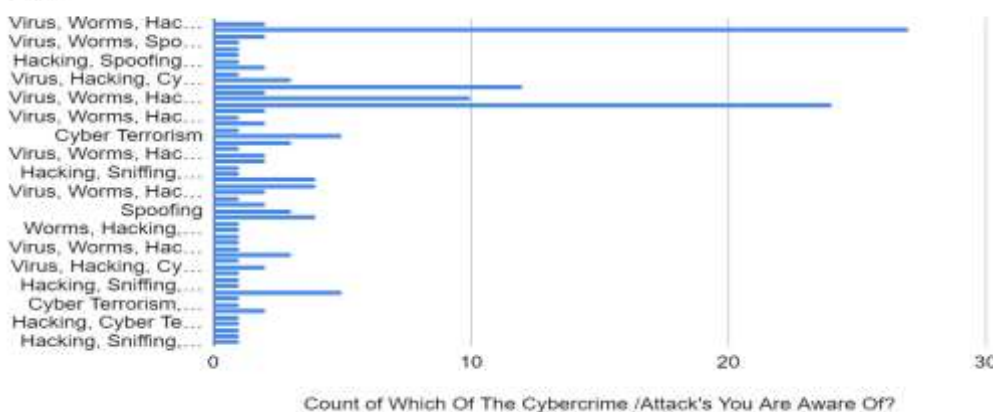


98% respondents use internet on their devices and only 1.2% people use internet occasionally.

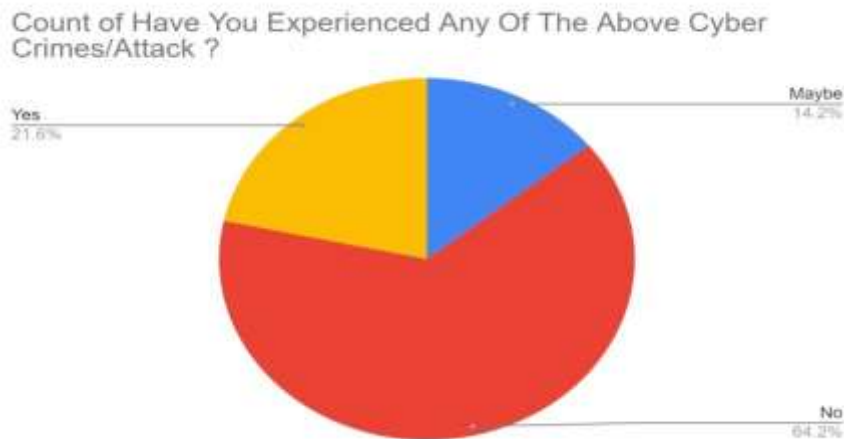
15% people are not familiar with the term ‘‘Cybercrime’’ and 68.9% are very familiar with the Term Cybercrime.



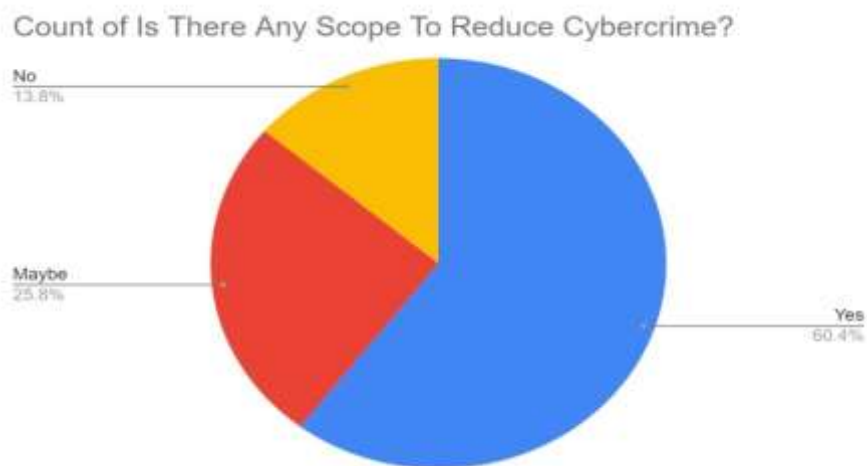
Count of Which Of The Cybercrime /Attack's You Are Aware Of?



Regarding awareness on various types of cybercrimes 64.4% people known about various types of crimes or attack's for e.g. Virus ,Worms, cyber stalking, Phishing, Identity theft, Cyber Bullying, mobile hacking.



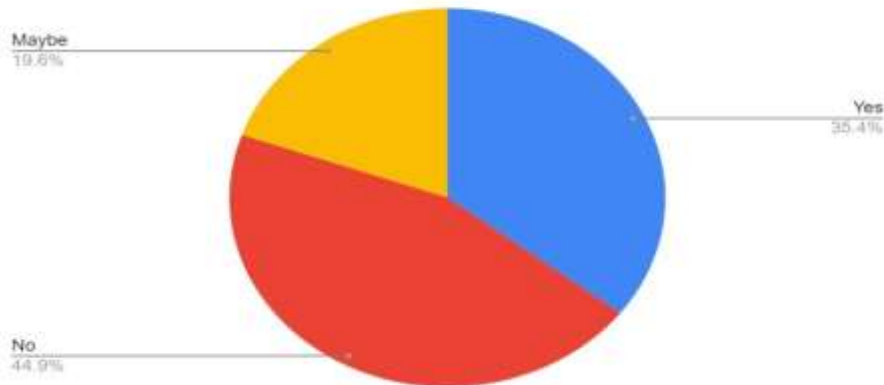
Only 21.6 people experienced cyber-attack and 64.2 % people aware about security, they well protected themselves from cyber-attack.



60.4% respondents agree that there is a scope to reduce cybercrime. Whereas, 25% people felt that there is no such a scope to reduce cybercrime.

70% people felt that the reason of cyber-attack due to unprotected data, unawareness about cybercrime, misuse of internet, not installing anti-virus software/application, share their personal details with unknown person, least security.

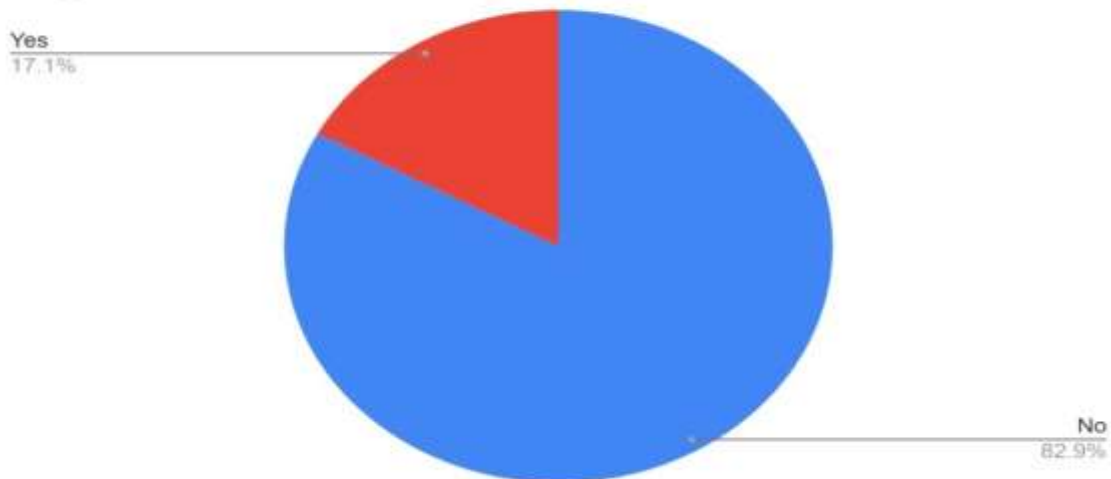
Count of Do you know about the existing Cyber Law IT ACT 2000 to overcome this Crime.



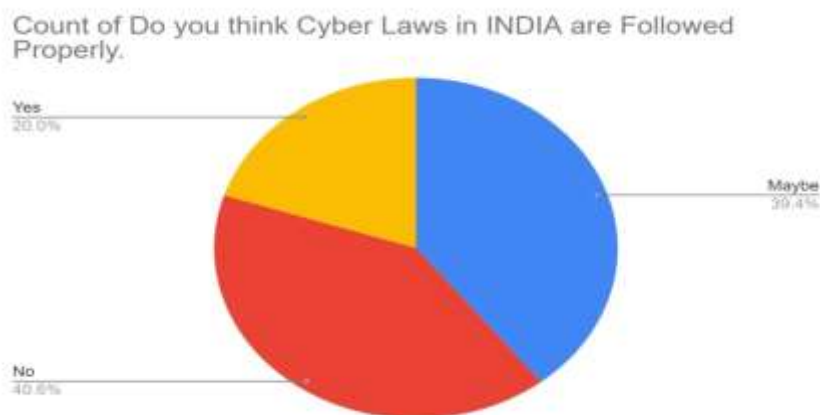
Only 35% people have referred to IT Act. 64% are aware that IT act deals with cybercrimes, but never referred it or read it. 19% IT Act, but not sure that cybercrimes are covered under it.

Remaining 44% have no idea about IT Act at all

Count of Have you ever lodged Cyber Crime Complaint on Register Portal?



82% people are may not aware about how to registered complaint on cybercrime portal or they may not affected by cybercrime. Only 17% people are aware about government Cybercrime complaint portal and if they face such kind of issues they have registered their compaint on portal.



The daily growth of cybercrimes, due to such issues the 40% people felt that, Cyber Laws in INDIA are not followed properly. Whereas 39% people felt that it may be followed properly.

Findings:

On the basis of interpretation of the data collected from the people, it is clear that the internet is most important for today's life. Most of the people are well known about Internet and their uses, 70% people are aware about Cyber Crime. The people well known about the new type of cybercrime attack and aware about how to take security and protect data from attacker. Awareness about the cyber laws people known the INDIA Cyber Law Act. The data was collected from more than 80% of under-graduate students who have experienced online scam and fraud. Around 88% of the people said that how to take security and protect our personal Data from others or unauthorized people. When it comes to the effectiveness of cyber law as to evaluation of people, around 35% people known about Existing Cyber Law IT Act 2000. Also as per evaluation if some person victimized by cybercrime they even did not known about

INDIA Gov. Complaint Portal. Only 17% people register their complaint on register portal. They think that 20 % of them cyber law in INDIA are followed effectively, but 40% of them don't believe the same. As a concerned, security as well as creating awareness about Cyber laws is very important for today's life. If someone in future may face this type of cyber-attack, they must be known about where to register the compliant and how to take necessary action among those attackers.



This study notes that there are several reasons why cybercriminals engage in crime. The main reason is to make quick money. Such groups are motivated by greed and often engage in electronic commerce, electronic banking, and fraud. Secondly, cybercrimes can be committed for prestige and recognition. Most of the perpetrators here are youngsters who want to attract attention and feel tough. They may be idealists who want to be in the spotlight but not hurt anyone. Thirdly, cybercrime can be committed to fighting for a cause that is key to the perpetrators' beliefs. In this situation, the perpetrators do not mind causing harm and destruction as long as their goals are accomplished.

Conclusion and Recommendations:

This research has pointed out that cybercrime is fast gaining ground in both developed and developing countries. The lead attempt of cybercrime are the youth who may have technical Experience, knowledge and experience to commit computer-related crimes. Find. This study discovered that conventional laws and policies are currently incapable of mitigating cybercrime cases. The awareness about Cyber Crime and Cyber Law among the people is very important. It is therefore crucial that they are reviewed in order to include new technological changes. It is also clear that computer crime is not considered a priority. Further, this study has shed light on the rapidness of cybercrime across the world. This paper recommends that similarly, the response to cybercrime need also be proportional. The Cyber law should be so strong and effectively implement so that the cyber attacker should fear of the consequences before doing such act.

References:

- Alghamdi, M. I. (June-2020). A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide. *International Journal of Engineering Research & Technology (IJERT)*.
- Animesh Sarmah, R. S. (June -2017). A brief study on Cyber Crime and Cyber Law's of India. *International Research Journal of Engineering and Technology (IRJET)* .
- Bhanu Sahu, N. S. (2013). *Identify Uncertainty of Cyber Crime and Cyber Laws*. Rajasthan, India: International Conference on Communication Systems and Network Technologies.
- J. (Nov-Dec 2016). A Study of Awareness About Cyber Laws for Indian Youth. *IJTSRD*.