JIGNASASTUDENTSTUDYPROJECT

Title:CYBERCRIMES

SUBMITTEDTO THECOMMISSIONEROF COLLEGIATEEDUCATION,HYD

Underthe

JIGNASA-2022-23

Government Degree College

Peddapalli

Submitted by

1. **T.ARUN KUMAR-BSCMPCS III YEAR -20077006468007**
2. **D.ARCHANA- BCOM II YEAR -210770064021008**
3. **S.SOUMYA-BCOM II YEAR- 210770064021049**
4. **K.AJAY-BSC BZC II YEAR-210770066101001**
5. **U.SRIKANTH - BSC MPCS II YEAR -210770064681017**

NameoftheSupervisor

R.SUNITHA

DEPARTMENT OF COMPUTERS

GDC PEDDAPALLI -TELANGANA

CONTENTS

DECLARATION

We do hereby declare that the work presented in this study project entitled **"CYBERCRIMES"** is an original one and has been carried out by us in the Department of Computers G D C Peddapalli, Dist: Peddapalli and has not been submitted either in part or in full for the award of any Degree or Diploma of any University earlier.

Date:15th December 2022

Place: Peddapalli

1.T.ARUN KUMAR-BSCMPCS III YEAR -20077006468007

2.D.ARCHANA- BCOM II YEAR -210770064021008

3.S.SOUMYA-BCOM II YEAR- 210770064021049

4.K.AJAY-BSC BZC II YEAR-210770066101001

5.U.SRIKANTH - BSC MPCS II YEAR -210770064681017

,

DEPARTMENT OF COMPUTERS

GOVERNMENT DEGREE COLLEGE, PEDDAPALLIDIST:

PEDDAPALLI

CERTIFICATE

This is to certify that the JIGNASA-Students' Study Project entitled **"CYBERCRIMES" is** an original one and has been carried out by **T.ARUN KUMAR-BSCMPCS III YEAR -20077006468007, D.ARCHANA- BCOM II YEAR -210770064021008, S.SOUMYA-BCOM II YEAR- 210770064021049, K.AJAY-BSC BZC II YEAR-210770066101001 and U.SRIKANTH - BSC MPCS II YEAR -210770064681017** in the Department of COMPUTERS, GOVERNMENT DEGREE COLLEGE ,PEDDAPALLIDist.: PEDDAPALLI, Telangana and completed under my supervision. It is a bona fide work done by them and has not been submitted elsewhere for the award of any Degree or Diploma or Competition. This study project is of the standard expected and I strongly recommend that it may be sent for evaluation.

Date: 15th December 2022

Place: Peddapalli.

R.Sunitha

Dept. of Computers

Study Project Supervisor

ACKNOWLEDGEMENT

We feel it great honor and proud privilege to extend our heartfelt gratitude to **Sri Navin Mittal IAS** garu, the Commissioner of Collegiate Education, Hyderabad, Telangana, for introducing such a wonderful, research oriented and skill development programme of JIGNASA to Degree College Students across the State of Telangana. Indeed, this programme develops the academic qualities, inquisitiveness, creative talent and the bent of research in the students. Thank you very much Sir for giving us an opportunity to undertake study projects under the **JIGNASA-Student Study Projects.** We owe a great debt of gratitude to **Sri P.Nithin**, beloved Principal of this College and the man of dedication and enthusiasm, for his constant motivation, encouragement for undertaking this study project and constructive suggestions for completion of this project. We feel immensely happy to extend deep sense of gratitude to our teacher and project supervisor Smt. **R.Sunitha**, dept. of Computers, G D C Peddapalli, who has guided us with meticulous care and scholarly advice. We thank all those who have directly and indirectly encouraged and supported us to carry out this study project.

From:

1.T.ARUN KUMAR-BSCMPCS III YEAR -20077006468007
2.D.ARCHANA- BCOM II YEAR -210770064021008
3.S.SOUMYA-BCOM II YEAR- 210770064021049
4.K.AJAY-BSC BZC II YEAR-210770066101001
5.U.SRIKANTH - BSC MPCS II YEAR -210770064681017

ABSTRACT:

The following students have gathered the information and continued their project with the effect of Cyber advancement in day-to-day life.

The literature is thoroughly refined by using the applicable knowledge. This project has given a scope of Cybercrime and safeguarding individuals/Organizations from its clutches.

The introduction part covers the scope of cybercrime and its effects. The second part deals with cybercrime, types of cybercrimes and cybercrime range. The later part of the project covers the crimes on the Internet and cybercriminal range. It concludes with case studies presented on the impact of cybercrimes related to “online fraud”, “cyber stalking”, “email-spoofing” and “e-mail-bombing” and method to counter the crime.

Today, Cybercrime has caused lot of damages to individuals, organizations and even the Government. Cybercrime detection methods and classification methods have come up with varying levels of success for preventing and protecting data from such attacks. Several laws and methods have been introduced in order to prevent cybercrime and the penalties are laid down to the criminals. However, the study shows that there are many countries facing this problem. The cybercrimes are of magnanimous value in western countries than in India.

The cybercrimes are on surge of late in India. The crime rate and types of it is increasing exponentially.

This project describes about the common areas where cybercrime usually occurs and the different types of cybercrimes that are committed today. The project also shows the studies made on e-mail related crimes as email is the most common medium through which the cybercrimes occur. In addition, some of the case studies related to cybercrimes are also laid down.

I. INTRODUCTION

Cybercrime, also known as computer crime, is the use of an instrument for illegal ends, such as committing fraud, trafficking in child porn the term "crime" is denoted as

- An unlawful act that is punishable by a state. However, certain purposes arenot defined by statute. A crime is also known as an offence or a criminal offense. It is harmful not only to some individuals but also to the community or the state.
- Cybercrime has nothing to do with the law.
- It involves computer or a computer network is essentially a collection of communicating nodes that aid in data transfer. The nodes at any given time could be a computer, a laptop, smart phones, etc. Cybercrime encompasses any criminal act dealing with computers and networks.
- It includes crime conducted through the Internet. The Internet is essentially a network of networks that is used for communication and data sharing all over the world.

With the advancement of Internet technologies like 2G, 3G & 4G, the global village is effectively sharing and communicating vital data across the network. However, there are some who are intentionally trying to track and extract vital and confidential information illegally for their personal use or for financial gain, and many more.

II .CYBERCRIME

Cybercrime encompasses a wide range of crimes, including stealing people's identities, fraud, and financial crimes.

Any crime involving a computer and the Internet is called "cybercrime." Some of the popular and alarming crimes in the cyber world are discussed below.

1. Financial Crimes

With the increasing demand for on-line banking, financial crimes have become very alarming. Financial crimes include credit card fraud, stealing money from online banks, etc. Criminals who commit credit card fraud frequently obtain information from their victims by impersonating government officials or people from financial institutions and requesting their credit card information. Victims fall prey to this without conducting proper due diligence and provide credit card information to these criminals. In this way, criminals may steal their identities, and the consequences are mostly financially damaging.

2. Cyber Pornography

Pornographic websites that allow the downloading of pornographic movies, videos, and pictures, as well as on-line pornography magazines (photos, writings, etc.), all fall under this category. "Computer pornography is a new horror" There are institutes that have conducted numerous studies and gathered evidence on child and computer pornography.

3. Drug Trafficking

Drug traffickers contribute significantly to cybercrime by selling narcotics while using cutting-edge encryption technologies. They arrange where and how to make the exchange, mostly using couriers. Since there is no personal communication between the buyer and dealer, these exchanges are more comfortable for intimidated people to use to buy illegal drugs and even other items.

4. CyberTerrorism

Terrorismactswhicharecommittedin cyberspace arecalledcyberterrorism. Cyberterrorismmayincludea simplebroadcast of information on the Internet about bomb attackswhich may happen ata particular time in the future.Cyber terrorists are people who threatenandcoerceanindividual,anorganizationorevena governmentbyattackingthemthroughcomputersandnetworksfortheirpersonal,politicalorsocialbenefits.

5. Online Gambling

On-line gambling offered by thousands of websites that have their servers hosted abroad.These websites are the one of the most important sites for money launderers.

6. CyberStalking

One of the prevalent forms of cybercrimes is Cyber stalking .Cyber stalking is following an individual's or organization's whereabouts on the Internet. These may include sending threatening or non-threatening messages on the victim's bulletin boards, which may be by social networking sites or even through e-mails.

This is basically a crime where the individual is constantly harassed by another individual example, sending constant mails to any individual with unsuitable contents and threat messages.

7. E-mail spoofing and phishing scams

Spoofing e-mails from known and unknown individuals is a common practise among cybercriminals.Email spoofing is the practise of sending an email from one source that appears to have come from another. Email spoofing is a very common cause of monetary damages.

The act of attempting to obtain vital information like passwords or credit card details by pretending to be a trustworthy entity in an electronic company is called "phishing." Phishing e-mails are likely to contain hyper-links to sites containing malware.

.

III. TYPES OF CYBERCRIME

There are different types of cybercrime today. But the eight most common ones are

1. Theft in the Services of Telecommunication

Individuals and criminal organisations can gain access to the switchboards of an organization's switchboard and obtain access to their dial-in or dial-out circuits. This allows them to make free calls to any local or distant number.

Theft of telecommunications services was one of the first forms of cybercrime and is a misdemeanour. The criminal is usually required to pay a fine and serve a short period of time in jail.

2. PiracyofTelecommunication

Digital technology today has allowed the perfect reproduction of prints and dissemination of graphics, sound, and other multimedia combinations. This has been an important concern for the owners of the copyrighted materials. When the creators of a particular work are not able to gain profit from their own creations, it leads to severe financial loss and has a great effect on creative efforts.

3. Dissemination of Offensive Materials

These are the materials that are thought to be objectionable and exist in cyberspace. It includes materials that are sexually explicit in nature, racist propaganda, explosive objects and devices, and codes for the fabrication of the incendiary devices.

Telecommunication services are also commonly used to harass, threaten, and intrude on communications, from phone calls to the contemporary manifestation of cyberstalking. Computer networks can also prove to be of use in further acts of extortion. These are the materials that are thought to be objectionable and exist in cyberspace. It includes materials that are sexually explicit in nature, racist propaganda, explosive objects and devices, and codes for the fabrication of the incendiary devices. Telecommunication services are also commonly used to harass, threaten, and intrude on communications, from phone calls to the contemporary manifestation of cyberstalking.

4. Laundering E-money and Evasion of Taxes

For quite a while, electronic funds transfers have been assisting in the hiding and transportation of crimes. The origin of ill-gotten gains will be greatly concealed by the emerging technologies of today.

Taxation authorities may easily conceal those legitimately derived incomes. Central bank supervision will be bypassed by the development of the informal banking institutions or the parallel banking systems. There is no separate law for this type of crime committed using a computer and a network, but it falls directly under the laws that cover these offences in general.

5.Extortion, terrorism, and electronic vandalism

Unlike in the past, the western industrial society now relies on complex data processing and telecommunications systems. Hampering or damaging these systems can lead to destructive consequences. Vandalism in general can be considered a denial-of-service attack, a botnet, or several other harmful network attacks. Extortion is the act of using money to demand the cessation of an attack or to refrain from initiating an attack. Computer vandalism penalties vary greatly depending on the amount of damage and loss caused, whereas extortion penalties are covered by the laws and rules of this type of felony.

6. Fraud in Sales and Investments

The use and development of applications in digital technology become more fraudulent and are bound to increase as electronic commerce becomes more prevalent.

Cyberspace has now availed itself of a lot of investment opportunities like bonds or stocks, the sale and leaseback of automatic teller machines, telephone lotteries, etc. Fraudsters may use a wide variety of tools to spread their information on the Internet. They may create fake websites to appear legal.

7. Illegal Interception of Telecoms Signals

The great and fast development in telecommunications allows for new opportunities for electronic eavesdropping. It includes everything from an individual's surveillance activities to industrial and political espionage. The existing laws do not prevent one from monitoring computer radiation from a distance.

8. Fraud in Transfer of Electronic Funds

Electronic transfer systems are proliferating, and the same goes for the risks that such transactions may be intercepted or diverted. There is no doubt that the electronic fund transfer system has gained sudden and wide acceptance globally. There is no doubt that the use of electronic fund transfer systems will increase the risk. The transfer of funds over the Internet may be diverted by the hackers. E-transfer is highly vulnerable in terms of crimes such as theft and fraud. There is no doubt that technological advancements in business services have benefited both businesses and consumers to a greater extent.Even though organisations are aware of the various types of cybercrime, it is extremely difficult for them to comprehend the capabilities of cybercriminals. It is indeed quite challenging for the organisations to understand the cybercriminals' next target and the value of their target. By the time the organisations realise they have been targeted, it is too late and the damage has been done. Despite efforts to prevent such cybercrimes, organisations continue to fall into the hands of cybercriminals.

IV. CRIMES ON THE INTERNET

Crimes committed on the Internet by using the Internet and by means of the same are mainly called "internet crimes. Cybercrime refers to the occurrence of harmful activities done with digital devices, mainly over the Internet. Cybercrime practically doesn't refer to the law, and it is the concept that is created to a greater extent by the media. In general, computer crime is a crime that encompasses crimes such as phishing, bank robbery, credit card fraud, child pornography, kidnapping of children by means of chat rooms, the creation or distribution of viruses, and so on. All these are computer-facilitated crimes. Some crimes that are committed on the Internet are exposed to the world, and some are hidden until they are perpetrated against someone or some company.

E-mail-related crimes:

Electronic mail has rapidly become the world's most preferred means of communication. Across the globe, millions of e-mail messages are sent and received every day. E-mail, like any other means of communication, is also being misused by criminals. It has become a powerful tool for criminals due to its ease, speed of transfer, and relative anonymity.

- **E-mail Spoofing:**

Electronic mail has rapidly become the world's most preferred means of communication. Across the globe, millions of e-mail messages are sent and received every day. E-mail, like any other means of communication, is also being misused by criminals. It has become a powerful tool for criminals due to its ease, speed of transfer, and relative anonymity.

- E-mail Defamation

Cyber defamation or cyber slander is often very dangerous and even fatal for anyone with even a rudimentary understanding of computers to become blackmailers, often by threatening their victims via e-mail.

- **E-mail Bombing**

E-mail accounts (in the case of an individual) or servers (in the case of a company) crashing due to a large amount of e-mails received by a victim is called "e-mail bombing". This can easily be done by subscribing the victim's e-mail address to a large number of mailing lists, which are special interest groups created to share and exchange data and information on a common topic with one

another through e-mail. Mailing lists can generate a sufficient amount of e-mail traffic daily, depending on the list. If a person unknowingly subscribes to multiple mailing lists, his incoming e-mail traffic becomes too large and can lead to the deletion of his account by his service provider.

- **E-mail Frauds:**

Financial crimes are commonly committed through e-mail spoofing. It is becoming easier to assume an identity as well as hide one's own identity. The criminal knows very well that there is a minimum chance of his being identified.

- **Spreading malicious codes:**

The most common and fastest ways to spread malicious codes are often e-mails. With the help of e-mail, a virus called "The Love Bug" spread to millions of computers within 36 hours of its release from the Philippines. Trojans, viruses, worms, and other computer contaminations are frequently packaged with e-greeting cards and e-mailed to unwary recipients.

- **Threats sent via e-mail:**

We find that the relative anonymity of e-mails offers technology-savvy criminals a useful tool. Anyone with little knowledge of how to send an e-mail can easily blackmail or threaten someone via e-mail without being identified.

V. CYBERCRIMINALS RANGE:

- **Kids (age group9-16)**

Although it is hard to believe, kids can also be cyber criminals knowingly or unknowingly. The most amateur hackers comprises of teenagers. To these teenagers, it appears to be a matter of pride to be able to hack in to a computer system or to a website. They may also commit the crimes without actually knowing that what they are doing is a crime.

- **Organized Hacktivists**

Hackers who come together with a particular motive are called hacktivists. These groups mostly operate on a political basis. While in other cases, their motives may be social activism or religious activism or any other.

- **Disgruntled Employees**

It is hard to imagine how spiteful disgruntled employees can become. Up until now, these displeased employees had the option of going on strike against their employers. But now, with the increase in dependence on computers and automation of processes, disgruntled employees can do a lot more harm to their employers by committing crimes via computers, which can bring their entire system down.

- **Professional Hackers**

Extensive computerization has led to the storage of information in electronic form in business organizations. Hackers are employed by rival organisations to steal other industrial information and secrets, which can prove beneficial for them. If hacking can retrieve the required information from rival companies, the fact that physical presence is required to gain access is considered unnecessary. This also increases the temptation for businesses to hire professional hackers to do their dirty work.

VI. CASE STUDY

Several cases of cybercrime have occurred recently in India. Some of these are described as follows:

Case I

An event occurred in April 2014 at Allahabad, India, where two undergraduate students, Vivek Kumar alias Kishan Dubey and Anand Mishra, were arrested for online fraud. These two students obtained a man named Mahmood's ATM password and committed credit card fraud amounting to Rs. 1.20 lakhs INR. The students were arrested and confessed to several of their frauds. According to the police, the two students would provide Delhi-based addresses for delivery of goods they had ordered online. Once the goods were delivered, they would sell them to gullible. This case had been registered under the IPC Act, sections 419 and 420, and under the IT Act, section 66.

Case II

On the context of Cyber Stalking, in 2013, Police at Cyderabad arrested a youth, N.Santosh Kumar alias Kiran, from Bangalore after he was charged for creating fake profile of a woman on Facebook. This youth also threatens the woman after she rejected his love proposal. Dejected ,he made the fake profile and also chats with others in her name. He also made threat calls and send messages to the victim's family. A complaint was lodged by the victim's brother on August, 2013 with Cyber Crime Police and the accused was arrested.

Case III

This case is on E-mail Spoofing, of late, one of the branch offices of the Global Trust Bank experienced a tough time. Many customers suddenly decided to with draw their money and further close their own bank accounts. On investigating, it was discovered that someone had sent spoofed emails to these customers and others too mentioning the bank was soon getting closed as it is having tough time financially.

Case IV

This case is about the Email bombing. This case speaks about a foreigner. He was staying in Simla, India for many years almost thirty years. He wanted to benefit from a scheme introduced by the Simla Housing Board to buy land at a lower price. However, his application was not accepted as they mentioned that the scheme is meant only for citizens of India. On this, this man decided to retaliate. Subsequently, he sent out thousands of mails to the Simla Housing Board and repeatedly kept sending e-mails till their servers crashed.

VII. CONCLUSION:

From this study made, it has been found that there are many ways and means through which an individual can commit crimes on cyber space. Cybercrimes are an offense and are punishable by law. Individual groups of individuals or organizations must safeguard itself from the notorious cybercrimes. Though it is vigilant the hands and means of cybercriminals prove to be dominant. The individuals and organizations falling prey to this menace inadvertently. Though there are no specific laws framed to punish the criminals they are sternly dealt with the laws in force as per the territory.

This project has given insight to the crimes of internet and computer one can be vigilant from these attacks by getting enlighten on the types and ways of cybercrimes.

The innocent are vulnerable to these attacks and there must be some mechanism either by self-help groups or from the government to make the public aware of these malpractices of cybercriminals and to protect themselves from such attacks.

It is therefore very important for every individual to be aware of these crimes and remain alert to avoid any loss. To ensure justice to the victims and punish the criminals, the judiciary has come up with some laws known as Cyber Laws. Hence, it is advisable to each and every individual to know these laws. Besides, the cybercrime cannot be simply called as a Technological problem. Instead, it is an approach based problem because it is not the computers that are harming and attacking the organizations instead it is the humans who are exploiting the technology to cause the damage.

Therefore, it is we who need to be alert to figure out the different approaches that such criminals can take. There is a need to have intellectual mindset to sense such situation that may lead to such damages. The solution to such crimes cannot be simply based on the technology. The technologies can just be one such weapon to track and put a brake to such activities to some extent.

Thank You.