WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cybercrime and Preventive Measures: Safeguarding Against Digital Threats

[1]Dr. Manisha Garg, [2]Dr. Rupinder Kaur, [3]Khushi Kalra

[1]Ass. Professor in Commerce, Government College for Women, Sirsa (Hry), **devishigarg@gmail.com.**

[2]Assit.Professor in Commerce, Government College for Women, Sirsa (Hry) **rupindertinna@gmail.com**.

[3]Student MA Economics Gokhale Institute of Politics and Economics Pune. **Khushikalra00@gmail.com**

ABSTRACT

Globally, there are more legal issues as a result of the rise in Internet traffic. The Internet is being used by cybercriminals to carry out a wide variety of illegal activities. Internet users battled spam emails, phishing calls, and emails requesting sensitive data such as their mobile number, bank account, address, etc. Both internet users and cybercrime have increased dramatically. Cybercrimes are crimes committed using a computer or computer network etc.

The prime target of the crime is ultimately computer. Because, a hacker takes commissions for it. Results from cybercrime are the securities loose and financial lose. The purpose of this study is to comprehend the various types of cybercrimes and cyber-attacks that occur today around the globe and to examine internet users' awareness of cybercrime. Despite a solid legal foundation and despite their silence, victims still do not receive justice. In today's society, objectifying people has become quite common. Because the criminals believe it to be a much simpler method with less punishment, cybercrime occurs. The government is also attempting to control cybercrimes. The government ought to impose stricter regulations on Internet service providers (ISPs). To catch the criminals, both the government and the populace should cooperate.

Keywords: Cyber-crime, Internet, Cyber Criminal, Cyber Security.

INTRODUCTION

Cybercrimes are on the rise along with the number of people using the internet. There is a chance that many of us will fall prey to the increasing number of criminals who are adept at using the Internet. "Illegal act in which a computer is a tool or a goal or both" is the definition of cybercrime. Cybercrime includes hacking a computer or computer network by another one. It may results in loosing once privacy, information and money.

Both internet users and cybercrime have significantly increased. Spam emails, phishing calls, and emails requesting sensitive information like a mobile number, bank account, address, etc. caused problems for internet users. Domestic and international cybercrime happens because of misusing of equipment in cyberspace. The most likely victims will be those who use vulnerable computers, email, social media, and the Internet. It shows that younger adults and adults over the age of 75 are typically the groups most susceptible to cybercrime.

The first polymorphic virus was introduced in 1992 along with the first cybercrime. In the history, Yahoo v. Akash Arorawas the first instances of cybercrime in India. This incident took place in 1999. From January to June of 2017, 27,482 instances of cybercrime were reported, by Indian Computer Emergency Response Team (CERT-In). Phishing, viruses or other malicious software, defacements, scrutinize, snooping, site intrusions, ransom ware, and denial-of-service attacks are a few of these. However, the public is unaware of all such varieties. Most people only have a basic understanding of hacking and viruses/worms.

Cyberspace, also referred to as the Web, is a dynamic and intangible environment. There are many different types of cybercrimes that take place every day. They are ignorant of phishing, cyber stalking, defamation, identity theft, etc. Today's world demands that we become knowledgeable about these online crimes. According to the study, 48% of respondents disclose personal information to people they don't know well. 55% of respondents concur that viruses frequently harm their PCs.

K. Jaishankar, he is the founding Father of Cyber Criminology, an academic sub-discipline of Criminology. First person, in 1981 who is convicted by cybercrime is Ian Murphy; also known as captain Zap for his followers. In the year 2021, many cities in India like Uttar Pradesh, Telangana and Karnataka are known for cybercrime cases. All India Institute of Medical Sciences has reported that hackers infiltrated of their services. So, in result data of million patients has to be compromised.

Data reported that, at least one cybercrime was reported in India every 10 minutes in the first half of 2017, which is more frequently than the every 12 minutes of 2016. 1.71 lakh cybercrimes have been reported in India during the last 3.5 years, and 27,482 have been reported so far this year. This suggests that the whole number will likely surpass 50,000 by the end of the year. Examination of data from 2013 to 2016 reveals that whereas viruses or malware accounted for 17.2% of cases, network scanning and probing accounted for 6.7% of all cases.

According to the most recent report from the National Crime Records Bureau (NCRB), 11,592 cases of cybercrimes overall up from 9622in 2014, a 20.5% increase. The most of these crimes have been reported in Uttar Pradesh, followed by Maharashtra and Karnataka. In today's scenario, world is facing the most difficult problem that is cybercrime. After using privacy, passwords, etc. still hackers access the account by illegally and private information of the users.

E-CRIMES OR CYBER CRIMES

Cyber-crime means misconduct that occurs with the help of a computer or web. When a computer is used as a tool, a target, or both, it is an illegal conduct. It consists of illegal actions taken while using electronic communication tools. Through the internet, something is being taken from the computer. In neither the Information Technology (IT) Act of 2000 nor the Indian Parliament has the phrase "cyber-crime" been defined. The IT Act of 2000 in India addresses crimes relating to cybercrime. The Indian Criminal Code (IPC), the IT Act, and other State Level Legislations are the three main categories under which cybercrimes are registered in India (SLL). A number of Cyber Cells have been established to handle only the cases where the crime rate in this area is rising quickly. Cybercriminals are using the Internet as a tool to engage in a wide variety of illegal activities. Cybercrime used to be primarily committed by lone individuals or small groups, but today there are many different types of cybercriminals, including professional hackers, organized hackers, kids and teenagers between the ages of 6 and 18, scammers, phishes, insiders, malware authors, spammers, etc.

Cybercrime against women is defined as "crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as the internet and mobile phones" by Debarati Halder and K.Jaishankar. Global legal issues now account for a higher percentage of Internet traffic. The Internet has grown tremendously, and with that growth have come more opportunities for cybercrime. In both the private and professional sectors, the threat of cybercrime is a constant and growing reality. Old crimes have a new look since the internet's invention. Enterprises frequently use computers not only to process information but also to gain a competitive and strategic advantage.

Objective of the Study

This essay makes the case that cyber- crime, also known as e-crime, represents a new breed of high-tech and business criminals, along with challenges and issues that may arise during prevention. The main purpose of this study is to comprehend the various types of **cybercrimes** and **cyber-attacks** that occur today around the globe and to examine internet users' awareness of cybercrime across a range of age groups and educational backgrounds. The objectives are decides as below:

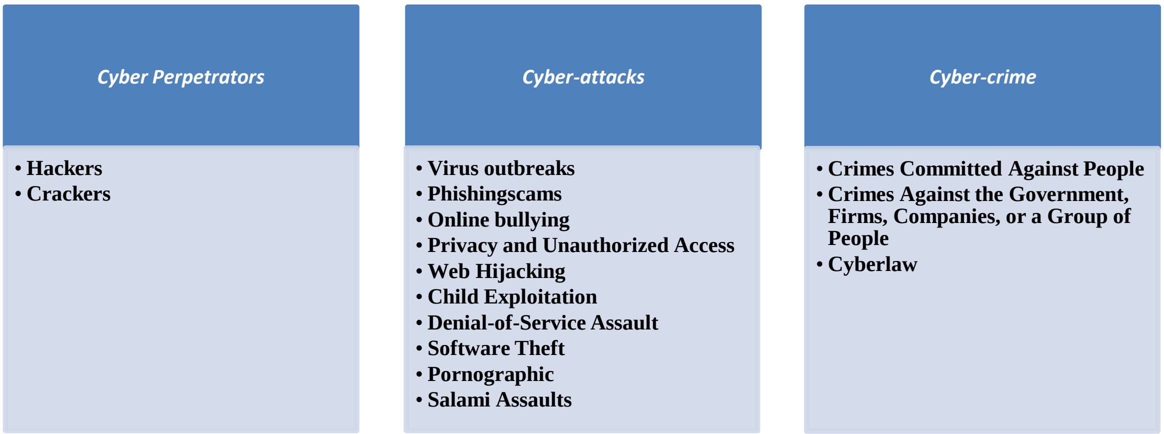
(1). To study about the cyber Perpetrators.

(2). A detail revision on Cyber-attracts.

(3). To know about the cyber-crime.

(4). To check the law and prevention against cyber-crime.

A detailed explanation of *Cyber Perpetrators, Cyber-crime and Cyber-attacks* are presented here under.



Cyber Perpetrators

- **Hackers**
- **Crackers**

Cyber-attacks

- **Virus outbreaks**
- **Phishingscams**
- **Online bullying**
- **Privacy and Unauthorized Access**
- **Web Hijacking**
- **Child Exploitation**
- **Denial-of-Service Assault**
- **Software Theft**
- **Pornographic**
- **Salami Assaults**

Cyber-crime

- **Crimes Committed Against People**
- **Crimes Against the Government, Firms, Companies, or a Group of People**
- **Cyberlaw**

(A)The Cyber Perpetrators

A. (1) Hackers

Hacker is common terminology and commonly applied to a "Computer use who intends to gain unauthorized access to a computer system". A person who by intentionally destroys or diminish the source or information of another person is known as hacker. In this process a hacker's desire to wrongly use the information of another person or public (IT Act 2000 section 66).

(2) Crackers

A "cracker" is a person who has malicious intentions. This phrase is required to distinguish "benign" hackers from those persons who have maliciously harm under attack computers, according to the Jargon Dictionary. For nefarious personal or political purposes, crackers deliberately damage computers, steal data from secure computers and disrupt networks.

(B) Cyber-attacks

It includes Virus outbreaks, Phishing connected to pandemics, Website fraud, Attacks using ransom ware, A rise in BEC assaults, Mobile malware, Cyber-terrorism, IOT and AI in online crime, Card Not Present Fraud, Data thefts etc.

(1) Virus outbreaks

Viruses are computer programs with the capacity to replicate themselves, spread to other programs, and infect them. Data on a computer is typically modified or deleted by viruses. Trojan horse is a program that mimics other behaviors.

(2) Phishing scams

One of the most common types of social engineering attacks is phishing, which seeks to trick unsuspecting users into disclosing personal information.

(3) Online bullying

Cyber bullying is the practice of a cybercriminal repeatedly harassing or threatening a victim while using online services.

(4) Privacy and Unauthorized Access

Any type of access without the consent of an authorized computer, computer system, or computer network is considered unauthorized access. Hacking is the term for breaking into a network or computer system without authorization. Piracy is any action taken to gain access to a computer or network. Hackers create their own computer programs or use pre-made ones to attack the target computer. They crave destruction and enjoy the rush it gives them. Some hackers compromise their own financial interests by stealing credit card data, moving funds from various bank accounts to their account, and then withdrawing the funds. The websites most targeted by hackers are those run by governments.

(5) Web Hijacking

Web Hijacking Taking complete control of another person's website is referred to as web hijacking. The website owner in this scenario forfeits control over his website and its contents.

(6) Child Exploitation

By disseminating pornographic material, pedophiles lure kids into their presence so they can have sex with them or take nude pictures of them engaging in sexual activity. Pedophiles sexually abuse children by using them as objects for sex or by taking their pictures so they can sell the images online.

(7) Denial-of-Service Assault

This type of attack deprives the victim of the services he is legally entitled to receive or provide by overloading his network bandwidth or overflowing his spam folder. This kind of attack aims to disable the network by saturating it with unneeded traffic.

(8) Software Theft

Software piracy is the term used to describe the illegal copying of original programs or the creation and distribution of products that are false copies of the originals. Theft of computer source code, copyright infringement, trademark infringement, and other similar offenses are also included in this category.

(9) Pornographic

Pornography refers to depicting sexual acts in order to arouse desire. Pornographic websites, computer-produced magazines, and Internet pornography are all included in the definition of pornography.

(10) Salami Assaults

Attacks of this nature are used to commit financial crimes. The goal is to make the changes so minor that they might not even be noticed in one instance.

(C) Cybercrime

Based on their target and effects, the major categories of cybercrime can be broadly divided into the following groups:

(1) Crimes Committed Against People

These crimes are committed with the intention of hurting specific people. These include child pornography, assault by threat, and denial of service attack, forgery, and phishing. They also include hacking, cracking, email harassment, cyber-stalking, cyber-bullying, defamation, and the spread of offensive material. Cybercrimes committed to harm a person's property include crimes against property. Intellectual property crimes, cyber-squatting, cyber-vandalism, computer hacking, computer vandalism, computer forgery, transmitting viruses and malicious software to damage information, Trojan horses, cyber trespass, Internet time thefts, robbery or stealing money while money transfers, etc. are some of the categories they fall under.

(2) Crimes against the Government, Firms, Companies, or a Group of People

These kinds of crimes include web jacking, salami attacks, logic bombs, possession of unauthorized information, distribution of pirated software, cyber terrorism, etc. These criminals want to terrorize the nation's residents. Crimes against Society: All of the aforementioned crimes have an impact on society as a whole, whether directly or indirectly. Therefore, all of these crimes—including pornography, online gambling, forgery, the sale of illegal goods, phishing, cyber terrorism, etc.—are included in this. Cybercriminals have seized this chance and profited from the widespread usage of the Internet by so many people. Due to widespread cyber security ignorance, there have been significant increases in cyber security threats during these pandemics. Cybercrime, or robbery carried out over a computer or the Internet, includes cyber theft. Due to the rise in cyber security fraud and crimes, the government is creating more precise regulations to safeguard citizens' interests and shield them from any unfavorable developments.

(3) Cyber law

Our heavy reliance on cyberspace, or the so-called Internet world, leads to cybercrime. Each of us has a responsibility to understand the fundamentals of cyber security. Cyber security is the term for the systems and procedures used to safeguard computers, webs, and data from unofficial entrance and online outbreaks from cybercriminals. The law on technological information, 2000, was approved by the Indian parliament with the goal of controlling criminal activity online and safeguarding the system of technological advancement. Preventing crimes and attacks is crucial, as is raising awareness of their different types. Global legal issues now account for a higher percentage of Internet traffic.

Cyber security laws protect access to information, privacy, communications, intellectual property (IP), and freedom of expression in relation to the use of the Internet, websites, email, computers, mobile phones, software, and hardware, such as data storage devices. They also help prevent or reduce large-scale damage from cyber-crime activities. The Information Technology Act of 2000 is the primary piece of legislation addressing the laws and policies governing the cyberspace; it advances the legal system in light of the evolving and modernized nature of the criminal justice system. The law's primary goals are to make electronic commerce legal and to make it easier to submit electronic registers to the government.

The Information Technology Bill was approved by the Indian Parliament's two houses in May 2000. The Information Technology Act of 2000 was created after the President gave his assent to the bill in August 2000. The IT Act of 2000 contains cyber laws. The purpose of this Act is to set up the legal framework for online shopping in India. Additionally, the cyber laws significantly affect India's new economy and e-businesses. Therefore, it's critical to comprehend the IT Act of 2000's various perspectives and what it has to offer. The IT Act of 2000 also targets to establish the lawful framework necessary to give all microelectronic proceedings and other events conducted via electrical means legal sanctity.

Defending against Cybercrime

To protect every employee from suffering a serious loss, it is imperative to provide the maximum amount of cyber security knowledge. Cyber laws vary by country and jurisdiction, are difficult to apply, and the penalties range from fines to imprisonment.

There are some safeguards, including

1. Always update your software.

2. Using antivirus software

3. Constant Password Changing

4. You must install a firewall and must not click any links in the email.

Get free anti-phishing add-ons, please.

6. Avoid providing personal information to websites you are not familiar with.

7. Refrain from opening shady attachments.

8. Keep Windows Firewall properly configured and active at all times.

9. Verify users and employ robust spam filters.

10. Try to use network and endpoint security tools.

11. Use encryption to protect the data while it is being transported.

12. Use secure authentication methods appropriately.

13. Double-check the spelling of URLs, HTTP addresses, and other online addresses.

Summary and Recommendations

Cybercrime is merely a reflection of what actually occurs in the real world. The distinction between the offline and online worlds is fading. There is a critical need for users to receive the best possible training and education. Such heinous crimes have been made possible by people's ignorance of technological advancements. People shouted from coast to coast. With millions of users on online platforms, the complaint processes have also lost their effectiveness.

"The law is not the only way to solve problems." Despite a solid legal foundation and despite their silence, victims still do not receive justice. In today's society, objectifying people has become quite common. Because the criminals believe it to be a much simpler method with less punishment, cybercrime occurs. The government is also attempting to control cybercrimes. Since Internet Service Providers (ISPs) have the complete record of the data that users accuse of being misused while browsing the web, the government should impose more stringent regulations on them. Not only the administration but public should also work hard to chase the crooks. Modern issues must be introduced in educational systems, and privacy policies on websites should be carefully considered. The need for people to take precautions arises. When using mobile devices like computers and phones, stay vigilant at all times. When sharing any personal information online, one should exercise caution.

References:

1. http://www.mondaq.com

2.https://telecom.economictimes.indiatimes.com/news

3.https://securitycommunity.tcs.com/infosecsoapbox/articles

4. http://www.helplinelaw.com/employment-criminaland-labour

5. Anuraj Singh (2007), Volume 05, Issue 06, PP. 11273- 11279.

6. AnimeshSarmahand and AmlanJyotiBaruah (2017), Volume 04, Issue 06, PP. 1633-1640.

7. J. Ahmed and Q. Tushar, \"Covid-19 Pandemic: A New Era of Cyber Security Threat and Holistic Approach to Overcome,\" 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020, pp. 1-5, doi: 10.1109/CSDE50874.2020.9411533.

8. L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider and G. Saldamli, \"Predicting and Preventing Cyber Attacks During COVID-19 Time Using Data Analysis and Proposed Secure IoT layered Model,\" 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA), 2020, pp. 113-118, doi:10.1109/MCNA50957.2020.9264301

9. S. Choudhary, P. P. Choudhary and S. Salve, \"A Study on Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks,\" 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 612-617, doi: 10.1109/ICICT43934.2018.9034445.

10. H. Zolfi, H. Ghorbani and M. H. Ahmadzadegan, \"Investigation and classification of cyber-crimes through IDS and SVM algorithm,\" 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 180-187, doi: 10.1109/I-SMAC47947.2023.9032536.

11. M. Arshey and K. S. Angel Viji, \"Thwarting Cyber Crime and Phishing Attacks with Machine Learning: A Study,\" 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 353-357, doi: 10.1109/ICACCS51430.2021.9441925.

12. S. Batra, M. Gupta, J. Singh, D. Srivastava and I. Aggarwal, \"An Empirical Study of Cybercrime and Its Preventions,\" 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, pp. 42-46, doi: 10.1109/PDGC50313.2020.9315785.

13.P. Datta, S. N. Panda, S. Tanwar and R. K. Kaushal, \"A Technical Review Report on Cyber Crimes in India,\" 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), 2020, pp. 269-275, doi: 10.1109/ESCI48226.2020.9167567.

14. http://www.google.com

https://www.ijlmh.com/paper/a-study-on-cyber-crime-and-its-legal-framework-in-india/

https://www.citefactor.org/journal/pdf/Cyber-Crime-in-India-An-Empirical-Study.pdf

https://www.ijraset.com/research-paper/types-of-cyber-crimes-and-cyber-attacks-today