Journal of Advanced Zoology

ISSN: 0253-7214
*Volume **43** Issue **S-1 Year 2022** Page **38:43***

Prevention Techniques on Cyber Crimes

Dr. Poonam P Nathani[1*], Dr. Sanjay S. Bang[2]

[1]*Assistant Professor, Dayanand College of Law, Latur, Email id - nathanipoonam30@gmail.com*
[2]*Associate Professor, Christ University, Lavasa, Email id - sanjay.satyanarayan@christuniversity.in*

**Corresponding author's E-mail: nathanipoonam30@gmail.com*

Article History

Received: 06 June 2023
Revised: 05 Sept 2023
Accepted: 16 Dec 2023

Abstract

With the increased use of computer and subsequent utility of internet cyber security has become a major problem. Due to technological advancement, we rely on internet and have absolute application for all the requirements in day-to-day life. Internet has given access to everything while sitting in a single location such as online shopping, online classes, online marketing, online jobs and everything. Cybercrimes are distinct from other crimes which occur in society. Cyber-crimes do not have territorial jurisdiction limits and faces are also unknown affecting every common man. Cybercrimes are generally associated with the use of computer, laptops mobile phones and other digital devices. It is also called as Digital Crime which is an offence targeted at computer data and its systems having unauthorized access, tempering, theft, modification, manipulations, corruption and so on are carried out. A digital or cybercrimes can occur when vulnerability is observed and is exploited in the system. Vulnerabilities are of various types that expose the system at risk, it may be Physical, Human, Hardware or software vulnerabilities. Generally, Cybercrimes are committed by highly skilled individuals or well competent and technically advanced organizations targeting the systems or data using viruses and other types of malwares or using digital devices to commit other ordinary crimes. This article on cybercrimes and preventive measures aims at focusing on the study of cybercrimes its types, legal challenges and very important how to mitigate its risk. It also aims at making the study on Cyber offences and Punishments as laid under the Information Technology Act 2000

Keywords: *Cyber Crimes, Digital Crimes, Information Technology Act, Computer, data protection*

1. Introduction

There are approximate 692.0 million internet users in india in January 2023 which stood at 48.7 percent however total of 1.10 billion cell connections were active January 2023 equivalent to 77.0 percent of the total population[1].. it offers the state of digitization of India. With the increasing use of digital tools, cybercrime is a major concern. The advancement of technology has made us depend on the internet for all our requirements. We can access everything while sitting on a computer, laptop or mobile phone. Everyday cyber world poses a new challenge before the world cybercrimes happening widely goes unreported by individuals or organizations, lack of awareness among the people and Authorities hampers the enforcement and implementation of the laws it borderless character assists the criminals by giving opportunities to do cybercrimes. These attacks occur where the data is digital, opportunity to wrongdoer and motive. It can be done by an individual to state-sponsored actors like intelligence agencies.[2] Cybercrime is a criminal activity that targets a computer, data, digital information, computer network or networked device.

What is Cyber Crime

Cybercrime is an illegal usage of any digital or electronic device or communication device to commit any illegal act or any criminal activity carried out over the internet with the motive to cause harm to individuals, business groups, or even governments. We cannot get any the exact definition of Cybercrime in any statute, even under the Information Technology Act, 2000 it is missing whereas in general this term means any illegal activity which is carried out with the help of internet or computers.

Dr. K. Jaishankar and Dr. Debarati Halder have defined cybercrimes as an offence committed against an individual or groups of people with the intention to cause harm to the reputation of the victim or cause physical or mental injury by directly or indirectly using the modern networks such as Internet (emails, Chat rooms, and online groups) and mobile phones through messages - SMS/MMS[3]

The oxford Dictionary defined the term cybercrime as "Criminal activities carried out by means of computers or the Internet[4]. Cybercrimes may be the species of which, genus is conventional crime and where the computer or other electronic device is an object or subject of the conduction of crime[5]

Professor S.T. Viswanathan said cybercrime is a crime where any illegal action is done by using a computer as a tool to do the crime the means or purpose of which is to influence the function of a computer. Secondly, he said any incident associated with computer technology causing harm to the victim with an intention to gain something 3 Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data[6] in general, cyber offences are viewed as the unlawful and illegal acts which are carried out in a sophisticated manner where either the computer is the tool or target.[7]

Vulnerabilities of the system or information and it's types

Often digital crimes are committed when a vulnerability is detected and observed in the system. Vulnerability is a weakness that exists in device or a group of devices which increases the risk of exploitation. Certain types of vulnerabilities expose the system to attack - Physical, human, hardware and software vulnerabilities.[8]

- Physical vulnerabilities include insecure devices, information or data that lead to physical theft, and exposure to adverse weather conditions causing damage.[9]
- Human vulnerabilities are caused by the direct action of authorized person. Such as staff and authorized persons discussing work or sensitive information at a public place. Here are some examples of human vulnerabilities -
  - Use or access of data files in insecure environments (outside the office using free wifi, at public places, taking data at home and so on.
  - Misplace or loss of devices, system, pen drive or data
  - Malicious attacking the system or disable security tools by an employee with criminal intention or to allow external unauthorized access.
  - Cheating by an employee
  - Leakage of sensitive information
  - Forget to shut down the system and access remained enabled [10]
- Hardware vulnerabilities occurs if weaknesses are in the hardware components of a digital or electronic system permitting unauthorized access directly through the hardware even from some remote location. Examples are system kept in open having excess of dust, humidity and heat affecting the performance of the device, old system or outdated hardware, manufacturing flaws in hardware or with configuration problem
- Software Vulnerabilities come through the software application where the standard protocols are not strictly followed during its development, or when we fail to keep security updates.[11]

Types of Cyber Crime

Basically, Cybercrime are of three major types depending on the targets such as Cybercrime against Person causing sexual, racial, religious or other type of harassment, cybercrimes against Property covers destruction of system, transmission of harmful virus, unauthorized access to the system or information causing trespass and against Government includes warfare, cyber terrorism, spying and so on

Cyber Crimes against persons are[12]:

- Cyber-Stalking means to create physical threat by repeated use of electronic communications through social media account, internet, e-mail, phones, text messages, or websites
- Dissemination of obscene material includes indecent exposure of child pornography, hosting or reflecting of website containing these prohibited materials.
- Defamation includes imputing any person to lower down the dignity by hacking his mail account

- Cracking means breaking down the computer systems without knowledge
- Hacking means unauthorized access over computer system to destroy the whole data as well as computer programs
- E-Mail Spoofing is a technique used in spam and phishing attacks to trick users to believe that a message has come from a person we either know or can trust them. It is misrepresented its origin.
- SMS Spoofing is a common method aiming to send links that will download malware into the devices. It is also a misrepresentation of the sender where it appears to be from someone we know
- Carding is a web security threat in which attackers use multiple, parallel attempts to authorize stolen credit card credentials
- Cheating & Fraud is caused by stealing password and data
- Child Pornography is a type of cybercrime to create or distribute the materials that sexually exploit children.

B. Crimes against Property[13]: As there is a development of e-commerce globally transactions are done through online mode increasing the risks of cybercrimes. Here are some examples of cybercrimes affecting the property of the person

- Under Intellectual Property Crimes victim is deprived completely or partially of his rights such as infringement of trademark, pirated copies, pirated software, theft of patent, designs and so on.
- Cyber Squatting means using or copying the domain name e.g gmail.com
- Cyber Vandalism means destroying the data when a network service is stopped or disrupted.
- Hacking Computer System means unauthorized control over online accounts, computers or the system
- Transmitting Virus is a mode to corrupt the system
- Cyber Trespass causes illegal access someone's computer without authorization
- Internet Time Thefts is also a type of cybercrime where the person gets access to someone else's ISP user ID and password, either by hacking or by gaining unauthorized access

Cyber Crimes against Government[14] There are certain offences done with the intention to threaten the governments to fulfill their illegal demands or to cause loss of data. The first example is Cyber Terrorism where sovereignty and integrity of the nation is endangered where attacks are on internet by distributed denial of service, hate e-mails and hate websites are circulated, sensitive computer networks are attacked. Cyber Warfare is another type of cybercrime used to disrupt the activities of government or the state for strategic or military purposes, it may be politically motivated activity. To destroy the data and official records many times there is distribution of pirated software. It is very easy to access any information by the terrorists with the aid of internet and to possess that information for political, religious, social, ideological objectives[15].

Legislative measures to curb the cyber crimes

The United Nations Commission on International Trade Law (UNCITRAL) realizing the impetus being given to digitalization and globalization adopted the Model Law on e-commerce in 1996, providing for recognition to electronic records giving it the same treatment like a paper communication and record. Therefore, in order to keep at pace with the requirements of the International Trading and also to allure industries into adopting this convenient way to transactions and storing data, the Information and Technology Act, 2000 was passed and to combat the increasing crimes related to internet The Information Technology Act, 2000 was enacted with the very objective to create an enabling environment for commercial use of I.T.

The IT Act specifies the acts which have been made punishable. Supporting to it Indian Penal Code has also been amended to curb cybercrimes[16]. Enactment of the Information Technology Act, 2000 (ITA), is a landmark moment marking India's commitment to recognize online securities to internet user and online commercial transactions. The Act 2000, has been amended in the year 2008 with the objective prescribed below[17] The various offenses related to cybercrimes which are punishable under the IT Act and the IPC are enumerated below: -

Information Technology Amendment Act, 2008

Chapter 11 of the Act,2000 covers the offences and the Penalties for cybercrimes. The cyber offences as mentioned under the Information Technology Act, 2000 have been listed below

- Section 65 of the Act deals with tampering with computer source documents which provides that any person who knowingly conceals, destroys or alters any computer source code when it is required to be kept or maintained, shall be punished with Imprisonment up to 3 years or fine up to Rs two lakhs or both
- Section 66 deals with computer related offences having punishment up to 3 years imprisonment or fine up to 5lakhs Rs.
- Section 66B gives punishment for dishonestly receiving stolen computer resource or communication device knowing the same is stolen device shall be punished for imprisonment up to three years or fine up to Rs.1 lakh
- Section 66C specify the punishment for identity theft, it says that if any person fraudulently makes use of the electronic signature, password, or any other unique identification feature of any other person, shall be punished up to three years of imprisonment
- Section 66D deals with punishment for cheating by personation by using computer resource - if any person, by means of any communication device cheats by personating will be punished by imprisonment up to 3 years and fine up to Rs. 1 lakh
- Punishment for violation of privacy is covered under section 66E providing that if any person intentionally captures or publishes the image of a private area of any person without his consent, violating the privacy, he shall be punished with imprisonment upto three years or fine up to Rs. 2 lakh or both
- Section 66Fof the Act, 2000 has set down the punishment for Cyber Terrorism. It says that a person commits the offence of cyber terrorism if he with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or intentionally accesses or penetrates a computer resource without authorization that is restricted for reasons of the security of the State or foreign relations which causes injury to the interests of the sovereignty and integrity and security of India, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise this offence is punishable up to Life Imprisonment
- Section 67 of the Act, 2000 states the punishment for publishing or transmitting obscene material in electronic form which is punishable Upon first conviction with imprisonment up to three years and fine up to Rs five lakhs; and upon second or subsequent conviction with imprisonment up to five years and fine up to Rs ten lakhs.
- Section 67A defines the punishment for publishing or transmitting of material containing sexually explicit act in electronic form. The punishment prescribed is - upon first conviction with
  imprisonment up to five years and fine up to Rs ten lakhs and upon second conviction with imprisonment up to seven years and fine up to Rs ten lakhs
- Section 67B provides for the punishment for publishing or transmitting of material depicting children in sexually explicit act in electronic form is punishable - Upon first conviction with imprisonment up to five years and fine up to Rs ten lakhs; and upon second or subsequent conviction with imprisonment up to seven years and fine up to Rs ten lakhs
- Section 67 C deals with the violating of the directions to preserve and retain the information by intermediaries which is punishable by imprisonment up to three years and fine
- Section 68 - Violating the directions of Controller by Certifying Authority or his employee is punishable to Imprisonment up to two years or fine up to Rs one lakh or both
- Section 70 deals with unauthorized access to a computer whose punishment is imprisonment up to ten years and fine
- Section 71 provides for penalty for misrepresentation. This section says that any person who makes any misrepresentation, or suppresses any material fact from the Certifying Authority for

obtaining any electronic signature certificate he shall be punished for a imprisonment which may extend to two years or with fine up to Rs. One lakh or with both

- Section 72 deals with Penalty for breach of confidentiality and privacy which says that if any person has secured access to any electronic record or other material without the consent of the person and discloses to any other person shall be punished with imprisonment which may extend to two years or with fine extending up to Rs. One lakh
- Section 72A contains with the punishment for disclosure of information in breach of lawful contract - person providing services under the terms of lawful contract, if, has secured access to any material containing personal information of another person discloses such material without the consent with intent to cause wrongful loss or wrongful gain shall be punished with imprisonment for a term extending three years or with fine up to Rs. Five lakhs or with both
- Section 73 prescribes the penalty for publishing Electronic Signature Certificate false in certain particulars where the person has knowledge that the certifying authority has not issued it or not accepted or it is revoked or suspended provision shall be punished with imprisonment up to two years or with fine up to Rs. one lakh or with both.
- another section 74 of the Act, 2000 lays down punishment for publication for fraudulent purpose. It says that any person, makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished up to 2 years or with fine extending one lakh Rs or with both.
- The provisions of this Act shall apply to all offences committed outside India by any person of any nationality However, for the act should involve a computer, computer system or computer network located in India, Section 75

Punishments for Cyber Crimes covered under IPC -

Section 383 of IPC Web-Jacking

Bogus websites, cyber frauds are covered under Section 420 of IPC

Section 463 - Forgery of electronic records and Email spoofing

Section 499 of IPC -Sending defamatory messages by email

Section 500 covers E-Mail Abuse

Section 503 - Sending threatening messages by email

How to protect against Cyber Crimes

Here are some measures which will prevent everyone from happening of cybercrimes which will protect our computer system, network, personal data and can prevent from cyber frauds -

Do not share the security keys and passwords with anyone

Use good quality antivirus and update regularly

Update software and operating system regularly

Scan detect and remove threats from devices when notification comes

Use of strong passwords prevent the happenings of crimes

Periodically change the passwords so that it cannot be guessed

Don’t record password anywhere

Think before opening the attachments in spam emails

Don’t accept fraud calls when notified

Don’t give response to links in spam emails by which computer get infected by malware virus

Unsafe websites should not be opened

Do not share personal information on social media or through sms unless secure

Never give out personal data over the phone or via email unless you are completely sure the line or email is secure.

Confirm that you are speaking to the person you know and trust

Regularly check bank statements

Before final click of payments confirm the amount and digits.

Contact companies directly about suspicious requests

If someone asks your personal information or bank details hang up.

Be mindful of which website URLs you visit

Keep an eye on the URLs you are clicking on.

Secure online transactions, ensure it is enabled before carrying out financial transactions online.

Always avoid sharing of any photograph online particularly to strangers

As you know that some financial loss has happen immediately contact cyber cell office near to your location. Take the help of proper authorities, follow the complaints and don't delay in filing complaint.

4. Conclusion

The Information Technology Act of 2000 covers the various cyber offences that the world is suffering from. Strict and stringent implementation of the Act may curb the cyber menace and the cyber space more safe and secure. This Act is generally linked with the Indian Penal Code, the Indian Evidence Act, 1872 and the Bankers Book Evidence Act 1891 for more comprehensive application. Alertness and awareness of the public in general is the key step to prevent cybercrimes. Increasing instances reminds us that it should be given as much importance as given to other or ordinary crime

References:

1. Information Technology Act, 2000
2. *Indian Evidence Act, 1872*
3. Indian Penal Code 1860
4. Psa Pillai's Criminal Law 14Th Edition, K I Vibhute, LexisNexis
5. Textbook On Indian Penal Code, K.D. Gaur, Universal, LexisNexis
6. S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary, 2001
7. COMMENTARY ON THE INFORMATION TECHNOLOGY ACT, Kush Kalra, Shikher Deep Aggarwal, Whitsmann Publishing Co., 2022
8. Information Technology Law and Practice- Cyber Laws and Laws Relating to E-Commerce, seventh Edn. 1 January 2021by Vakul Sharma and Seema Sharma, , Universal, LexisNexis
9. www.techtarget.com/searchsecurity/definition/cybercrime
10. inflibnet.ac.in/
11. www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html
12. http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf, Profiling a Cyber Criminal Rashmi SarohaDepartment of Psychology, University of Delhi, New Delhi, India. International Journal of Information and Computation Technology.
13. https://datareportal.com/reports/digital-2023-india