# CYBER CRIMES: TYPES, PATTERNS AND PROSPECTS

**Tanaya Wageshwari,** Assistant Professor, RNB Global University, Bikaner, Rajasthan

**Abstract:**

With the rising utilization of computers in the public eye, cybercrime has turned into a significant issue. Cyber Crime is certainly not an old kind of crime to the world. It is characterized as any crime which happens on or over the mode of computers or internet or all the other technologies as recognized by Information Technology Act.

The headway of innovation has made man reliant upon internet for every one of his requirements. Internet has given man admittance to all that while sitting at one spot. Interpersonal interaction, internet based shopping and contemplating, online positions, and each potential things that Man can imagine should be possible with the help of internet.

This article attempts to study a brief presentation of cybercrime, different types, and other concepts such as- Cyber pornography, Cyber stalking, Cyber terrorism, Hacking, Identity theft, etc. Through this research study, the researcher has discussed about the patterns and prospects towards the concept of Cyber Crime. This paper discusses about various offences under this head which are against the persons as well as property. This research study provides the legislative provisions about the concept of cyber-crime and its applications.

**Key words:** Cyber Crime, Digital lawbreakers, Information Technology Act, Internet Shopping.

## I. INTRODUCTION

Cyber-crime is basically a crime which has been done with the help of Information and Communication Technology. Cybercrime is a wide term that is utilized to characterize crime in which computers or computer networks are a device, an objective, or a position of crime and incorporate everything from electronic wracking to disavowal of administration assaults. A general term covers wrongdoings like phishing, credit card frauds, bank burglary, unlawful downloading, modern surveillance, child pornography, seizing youngsters through discussion boards, tricks, digital psychological oppression, creation as well as dissemination of viruses, spam, etc.

It additionally covers that conventional violations in which computers or networks are utilized to empower the unlawful activity. Cyber-crime is expanding step by step, these days it has turned into another design to earn money by fraud calls or to take revenge through hacking other accounts.

Cybercrime is crime that either targets or uses a PC, a PC organization or an arranged gadget. The overwhelming majority cybercrime is perpetrated by cybercriminals or programmers who need to bring in cash. Cybercrime is completed by people or associations. Some cybercriminals are coordinated, utilize progressed methods and are exceptionally in fact talented. Others are fledgling programmers. Once in a while, cybercrime means to harm PCs because of reasons other than benefit. These could be political or individual. Cybercrime is a perilous wrongdoing including PCs or advanced gadgets, in which a PC can be either an objective of the wrongdoing, a device of the wrongdoing or contain proof of the wrongdoing. Cybercrime essentially characterized as any crime that happens over the Web. There are numerous models like extortion, malware, for example, viruses, data fraud and digital following.

In present climate, since most data handling relies upon the utilization of data innovation, the control, avoidance and examination of digital exercises is imperative to the outcome of the Associations, Government's organizations and people. The obtainment and support of exceptionally ability cybercrime master by Government and Business Endeavors can't be overstated. Prior, cybercrime was carried out basically by people or little gatherings. As of now, it is seen that there is profoundly perplexing cybercriminal networks unite people at worldwide level continuously to perpetrate violations. Today, hoodlums that enjoy cybercrimes are not roused by self-image or ability. All things

 

being equal, they need to utilize their insight to instantly acquire benefits. They are utilizing their capacity to cut, bamboozle and take advantage of individuals as they find it simple to create cash without accomplishing a fair work. Cybercrimes have become significant danger today.

## II. DEFINITIONS OF CYBER CRIME

In a very simple manner we can say that cyber-crime is unlawful demonstrations wherein the PC is either a device or an objective or both. Cyber-crime can include crimes that are customary in nature, for example, robbery, extortion, imitation, criticism and wickedness, which are all dependent upon the Indian Penal Code. Cybercrime is the dark side of technology. The word 'cybercrime' is not mentioned in the Information Technology Act 2000 or any other law of the country. Cybercrime is no different than traditional crime. The only difference is that computer technology is involved in cybercrime.
Cybercrime is defined as an action in which the computer or network is utilized as a device for Crime. Cybercrimes can be recognized as unlawful way of behaving coordinated through electronic tasks that focus on the security of PC frameworks and the information handled by them. Cybercrime, from a more extensive perspective, are a PC related wrongdoing, any unlawful way of behaving carried out through, or corresponding to, a computer or network, including such violations as unlawful belonging and offering or dispersing data through a computer or network.

## III. TYPES OF CYBER CRIME

Cybercrimes against people, property and government.

- Cybercrimes against people incorporate different wrongdoings, including the transmission of obscene messages, email, digital tormenting, and digital following.
- The second class of digital wrongdoings is digital violations against associations or a wide range of resources. These wrongdoings incorporate unlawful and unapproved PC intruding and sending significant and basic data outside the association which can make incredible harm the association.
- The third classification of cybercrimes connects with cybercrimes against the government including cyber terrorism.

### *a) Cyber Pornography*

Cyber Pornography implies the distributing, disseminating or planning porn by utilizing the internet. The innovation has its upsides and downsides and cyber pornography is the consequence of the headway of innovation. With the simple accessibility of the Web, individuals can now see large number of pornography on their mobiles or PCs, they even approach transfer explicit substance on the web.
Avinash Bajaj v. State (N.C.T.) of Delhi ; An obscene video titled “DSP Girls having fun” was uploaded by a user (Ravi Raj, a student of IIT Kharagpur) on the website bazee.com. The MMS was posted on the website around 8:30 pm of 27 November 2004, which was deactivated around 10 am on 29 November 2004.An F.I.R was also lodged against the bazee.com for putting on sale the obscene material. The CEO of bazee.com, Avinash Bajaj was arrested by the police under Section 67 of the IT Act. Since Ravi Raj (the user who uploaded the MMS) absconded, Avinash Bajaj file a petition, seeking the quashing of criminal proceedings. The CEO of bazee.com was released on bail subject to furnishing of two securities in the sum of ₹1, 00,000. The accused was also directed not to leave India without the permission of the Court. He was also directed to participate and assist in the partnership .

### *b) Cyber Stalking*

The main term stalking means to reliably following a specific individual over an extensive stretch of time. This movement likewise includes the badgering or compromising way of behaving. The stalker reliably following an individual wherever at home, market and so forth, and the stalker likewise compromise that individual by more than once sending the messages, doing clear calls.
However, in the cyber stalking there is a utilization of the web or some other electronic media by which the correspondence should be possible through the Messages or SMS to follow that individual. A cyber

 

stalker's thoroughly depends upon the subtlety given by the web, which permits them to follow their casualty without being distinguished. The digital following is entirely unexpected from the spamming of the messages by the spammer.
Cyber stalking is a kind of a wrongdoing. In the cyber stalking there is a contribution of two people First and foremost, the stalker is otherwise called assailant who do the wrongdoing and besides, the Casualty who is bugged by that stalker. Cyber stalking is otherwise called cybercrime. Digital which is connected with the web and the following means to perusing anybody's internet based history with the assistance of any virtual entertainment or in different sites to realize about that specific individual is term as stalking .

***c) Cyber Terrorism***

Cyberterrorism is many times characterized as any planned, politically persuaded assault against data frameworks, projects and information that undermines viciousness or results in brutality. The definition is at times extended to incorporate any digital assault that threatens or creates dread in the objective populace. Assailants frequently do this by harming or disturbing basic framework.
Instances of cyberterrorism incorporate the accompanying :
Interference of critical destinations. The objective here is to unveil trouble or stop traffic to destinations containing content the software engineers can't resist the urge to go against.
Unapproved access. Aggressors often mean to disable or modify correspondences that control military or other fundamental development.
Interference of essential establishment systems. Risk performers endeavor to cripple or disturb metropolitan networks, cause an overall prosperity crisis, imperil public security or cause enormous craze and fatalities. For example, cyberterrorists could zero in on a water treatment plant, cause a common power outage or upset a pipeline, petrol handling plant or profound oil penetrating movement.
Cyberespionage. States oftentimes complete or uphold cyberespionage attacks. They plan to watch out for rival nations and aggregate knowledge, similar to troop regions or military frameworks.

***d) Identity Theft***

Identity theft generally get individual data, for example, passwords, ID numbers, MasterCard numbers or government managed retirement numbers, and abuse them to act deceitfully in the casualty's name. These delicate subtleties can be utilized for different unlawful purposes including applying for credits, making on the web buys, or getting to casualty's clinical and monetary information.

***e) Cyber Bullying***

Cyberbullying is tormenting that happens over advanced gadgets like mobile phones, PCs, and tablets. Cyberbullying can happen through SMS, Text, and applications, or online in web-based entertainment, discussions, or gaming where individuals can see, partake in, or share content. Cyberbullying incorporates sending, posting, or sharing negative, destructive, misleading, or mean substance about another person. It can incorporate sharing individual or confidential data about another person causing shame or embarrassment. Some cyberbullying goes too far into unlawful or criminal way of behaving .
The most well-known spots where cyberbullying happens are:

- Online Entertainment, like Facebook, Instagram, Snapchat, and Tik Tok
- Text endlessly informing applications on versatile or tablet gadgets
- Texting, direct informing, and web based talking over the web
- Online discussions, discussion channels, and message sheets, like Reddit
- Email
- Web based gaming networks

***f) Cyber Sexual Defamation and Harassment***

Cyber sexual harassment includes the activities of an individual or people towards the casualty in the internet which causes profound trouble, mental provocation, orientation badgering, intrusion of security and so on. The harassers could affect dread of actual mischief, give dangers, post something disparaging about the victim. This could likewise prompt imitating casualties in obscene locales. These

 

demonstrations once in a while will generally seem like tormenting however not provocation. There is a slim line of differentiation between them which will in general obscure when the foundation of such a demonstration is the cyber worlds or computerized world. In any case, both the ways of behaving are improper and thus, the law should be made in such a manner to generally rebuff it. Recognizing acts is by all accounts to no end when it is an instance of the internet provocation, yet can find lasting success whenever recognized based on designated crowd.

## IV. PATTERNS & PROSPECTS

Cybercrime is having various patterns and their prospects. Whatever patterns are there for the cybercrime or we can say cyber-attacks, there will be prospects of all these patterns and so that it will have a bad effect upon the society. There are a few patterns of cybercrimes; the most widely recognized ones are Hacking, Denial of Service Attack, Software Piracy, Phishing, and Spoofing. Also we can go through other patterns of cybercrime, such as- email cheats, online entertainment fakes, banking fakes, ransomware assaults, digital reconnaissance, fraud, clickjacking, spyware, and so forth.

### *a) Hacking*

Hacking first showed up as a term during the 1970s however turned out to be more famous through the following ten years. An article in a 1980 release of Brain science today ran the title "The Programmer Papers" in an investigation of PC uses habit-forming nature. After two years, two motion pictures, Tron and Wargames, were delivered, in which the lead characters set about hacking into PC frameworks, which acquainted the idea of hacking with a wide crowd and as a potential public safety risk.

Sufficiently sure, soon thereafter, a gathering of teens broke the PC frameworks of significant associations like Los Alamos Public Lab, Security Pacific Bank, and Sloan-Kettering Malignant growth Community. A Newsweek article covering the occasion turned into the first to utilize "programmer" in the negative light it currently holds. This occasion likewise drove Congress to pass a few bills around PC violations, however that didn't stop the quantity of high-profile assaults on corporate and government frameworks. Obviously, the idea of hacking has spiraled with the arrival of the public web, which has prompted undeniably more open doors and more worthwhile compensations for hacking movement. This saw strategies develop and increment in refinement and brought forth a great many sorts of hacking and programmers .

Hacking alludes to exercises that try to think twice about gadgets, like PCs, cell phones, tablets, and, surprisingly, whole organizations. And keeping in mind that hacking could not necessarily in every case be for pernicious purposes, these days most references to hacking, and programmers, portray it/them as unlawful movement by cybercriminals — propelled by monetary profit, fight, data gathering (spying), and, surprisingly, only for the "good times" of the test.

Hacking is ordinarily specialized in nature (like making malvertising that stores malware in a drive-by assault requiring no client communication). In any case, programmers can likewise utilize brain research to fool the client into tapping on a malignant connection or giving individual information. These strategies are alluded to as "social designing." As a matter of fact, it's precise to portray hacking as a general umbrella term for movement behind the overwhelming majority of the malware and pernicious cyberattacks on the figuring public, organizations, and states.

### *b) Denial of Service Attack*

A Denial of Service (DoS) assault is an assault intended to close down a machine or organization, making it out of reach to its expected clients. DoS assaults achieve this by flooding the objective with traffic, or sending it data that sets off an accident. In the two occurrences, the DoS assault denies genuine clients (for example workers, individuals, or record holders) of the help or asset they anticipated. Survivors of DoS goes after frequently target web servers of high-profile associations like banking, business, and media organizations, or government and exchange associations. However DoS assaults don't commonly bring about the burglary or loss of huge data or different resources, they can cost the casualty a lot of time and cash to deal with.

 

There are two general techniques for DoS assaults: flooding administrations or crashing administrations. Flood assaults happen when the framework gets an excessive amount of traffic for the server to support, making them delayed down and ultimately stop. Well known flood assaults include:
***Support flood assaults -*** the most widely recognized DoS assault. The idea is to send more traffic to an organization address than the software engineers have fabricated the framework to deal with. It incorporates the assaults recorded underneath, notwithstanding others that are intended to take advantage of bugs well defined for specific applications or organizations
***ICMP flood -*** influences misconfigured network gadgets by sending caricature parcels that ping each PC on the designated network, rather than only one explicit machine. The organization is then set off to enhance the traffic. This assault is otherwise called the smurf assault or ping of death.
***SYN flood -*** sends a solicitation to interface with a server, however never finishes the handshake. Go on until all open ports are immersed with solicitations and none are accessible for authentic clients to associate with.
Different DoS goes after just endeavor weaknesses that make the objective framework or administration crash. In these assaults, input is sent that exploits bugs in the objective that hence crash or seriously undermine the framework, so it can't be gotten to or utilized.
An extra kind of DoS assault is the Distributed Denial of Service (DDoS) attack. A DDoS assault happens when numerous frameworks organize a synchronized DoS assault to a solitary objective. The fundamental contrast is that as opposed to being gone after from one area, the objective is gone after from numerous areas immediately.

***c) Software Piracy***

Software piracy is the demonstration of taking programming that is legitimately safeguarded. This taking incorporates replicating, circulating, altering or selling the product. Copyright laws were originally put into place so that the people who develop software (programmers, writers, graphic artists, etc.) would get the appropriate credit and remuneration for their work. At the point when programming robbery happens, pay is taken from these copyright holders.
Consequences of software piracy are:

- Expanded possibilities that the product will glitch or come up short
- Relinquished admittance to help for the program, for example, preparing, updates, client service and bug fixes
- No guarantee and the product can't be refreshed
- Expanded hazard of contaminating your PC with malware, infections or adware
- Slowed down PC
- Legitimate repercussions because of copyright encroachment

***d) Phishing***

Phishing is a sort of social engineering assault frequently used to take client information, including login certifications and MasterCard numbers. It happens when an aggressor, taking on the appearance of a confided in substance, hoodwinks a casualty into opening an email, text, or instant message. The beneficiary is then fooled into clicking a pernicious connection, which can prompt the establishment of malware, the freezing of the framework as a component of a ransomware assault or the noteworthy of delicate data.
An assault can have destroying results. For people, this incorporates unapproved buys, the taking of assets, or distinguish robbery.
Besides, phishing is in many cases used to acquire a traction in corporate or legislative organizations as a piece of a bigger assault, like a high level tireless danger (Well-suited) occasion. In this last situation, representatives are compromised to sidestep security edges, disperse malware inside a shut climate, or gain restricted admittance to get information.
An association surrendering to such an assault regularly supports serious monetary misfortunes as well as declining portion of the overall industry, notoriety, and customer trust. Contingent upon scope, a

 

phishing endeavor could grow into a security occurrence from which a business will struggle with recuperating.

***e) Spoofing***

In online protection, 'spoofing' is when fraudsters profess to be some other person or thing to win an individual's trust. The inspiration is as a rule to get close enough to frameworks, take information, take cash, or spread malware. Parodying is a wide term for the kind of conduct that includes a cybercriminal taking on the appearance of a confided in substance or gadget to inspire you to do something helpful to the programmer — and negative to you. Any time an internet based trickster masks their way of life as something different, it's spoofing. Spoofing can apply to a scope of correspondence channels and can include various degrees of specialized intricacy. Ridiculing assaults normally include a component of social designing, where tricksters mentally control their casualties by playing on human weaknesses like trepidation, ravenousness, or absence of specialized information.

## V. LEGISLATIVE PROVISIONS

Cybercrimes are again class of violations which are expanding step by step because of broad utilization of web nowadays. To battle the violations connected with web The Data Innovation Act, 2000 was ordered with prime goal to establish an empowering climate for business utilization of I.T. The IT Act determines the demonstrations which have been made culpable. The Indian penal Code, 1860 has likewise been changed to take into its domain digital violations.

The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

1. Cybercrimes under the IT Act :

a. Tampering with Computer source documents - Sec.65
b. Hacking with Computer systems, Data alteration - Sec.66
c. Publishing obscene information - Sec.67
d. Un-authorized access to protected system Sec.70
e. Breach of Confidentiality and Privacy - Sec.72
f. Publishing false digital signature certificates - Sec.73

2. Cyber Crimes under IPC :

a. Sending threatening messages by email - Sec 503 IPC
b. Sending defamatory messages by email - Sec 499 IPC
c. Forgery of electronic records - Sec 463 IPC
d. Bogus websites, cyber frauds - Sec 420 IPC
e. Email spoofing - Sec 463 IPC
f. Web-Jacking - Sec. 383 IPC
g. E-Mail Abuse - Sec.500 IPC

3. Cyber Crimes under the Special Acts:

1. Online sale of Drugs
2. Online sale of Arms

## VI. CONCLUSION & SUGGESTIONS

Cybercrime in India has been quickly developing starting from the beginning of the mechanical period. Consistently, as a matter of fact, you get to hear various stunts, tricks and numerous different offenses being committed on the internet. There are many sorts of digital wrongdoing in India that have proactively been recorded under the Data Innovation Act, 2000, recommending different kinds of violations. Likewise to adhere to the rules of digital wrongdoing act in India, in significant urban communities, numerous digital wrongdoing cells in India have been set up.

With the headway of innovation, ongoing instances of digital wrongdoing in India has additionally expanded. Today, numerous violations like abducting, extortion, hacking, and information robbery are being dedicated with the assistance of web. Hoodlums who perform such exercises are frequently

 

alluded to as "programmers". Large numbers of the digital wrongdoing cases in India are enrolled under the IT Act.

Digitalization is unrestrained nowadays and the Web has made life more straightforward for everyone, with everything simply a tick away. From middle class wrongdoings to assaults by fear monger associations, the quantity of digital violations in India has additionally expanded. It has made man subject to the innovation for every last essential need. Today each need is covered internet based like internet shopping, requesting food, and web based gaming, making installments and so on.

To deal with the situation of cybercrime effectively, one requirements to lay out complex public-private joint efforts between policing, the data innovation industry, data security associations, web organizations, and monetary establishments.

In contrast to this present reality, digital crooks don't battle each other for matchless quality or control. All things considered, they cooperate to work on their abilities and even assist with outing each other with new open doors. Thus, the typical strategies for battling wrongdoing can't be utilized against digital violations in India.

Utilize Solid Passwords: Utilize the different secret key and username mixes for various records and oppose the compulsion to get them on paper.

Keep your online entertainment accounts hidden: Be certain that you keep your long range interpersonal communication profiles (Facebook, Twitter, YouTube, and so forth) private. Make certain to actually take a look at your security settings. Watch out for what data you post on the web. When it is on the Web it is there for eternity.

Secure your Cell phones: Many individuals don't know that their cell phones are likewise powerless against malignant programming, for example, PC infections and programmers. Make certain to download applications just from confided in sources. It is likewise urgent that you stay up with the latest. Make certain to introduce hostile to infection programming and to utilize a solid lock screen too. If not, anybody can get to all your own data on your telephone on the off chance that you lose it or even put it down for a couple of seconds. Somebody actually might introduce pernicious programming that could follow all your developments through your GPS.

Safeguard your information: Safeguard your information by involving encryption for your most delicate documents such monetary records and expense forms.

Safeguard your character on the web: With regards to safeguarding your personality online being excessively wary than not mindful enough is better. It is important that you be careful while giving out private ID, for example, your name, address, telephone number and additionally monetary data on the Web. Be sure to ensure sites are secure while making on the web buys, and so on. This incorporates empowering your security settings while utilizing/getting to informal communication destinations.

Keep your PC current with the most recent fixes and updates: One of the most incredible ways of getting assailants far from your PC is to apply patches and other programming fixes when they become accessible. By consistently refreshing your PC, you block aggressors from having the option to exploit programming blemishes (weaknesses) that they could somehow use to break into your framework.

Safeguard your PC with security programming: A few kinds of safety programming are fundamental for essential internet based security. Security programming fundamentals incorporate firewall and antivirus programs. A firewall is normally your PC's most memorable line of safeguard. It controls who and what can speak with your PC on the web. You could consider a firewall a kind of "cop" that observes every one of the information endeavoring to stream all through your PC on the Web, permitting correspondences that it knows are protected and hindering "terrible" traffic, for example, assaults from truly arriving at your PC.

 