# Cybercrime around the world: an analysis

**Rohit Saini**, Ph.D Research Scholar
Department of Law, Pandit Deendayal Upadhyaya Shekhwati University, Sikar, Rajsthan-332024

**ABSTRACT**

Due to the pervasive use of computers in daily life, cybercrime has become a significant issue. Man now solely relies on the internet because of technological advancements. Thanks to the internet, a person can now access anything while seated in one place. The internet can be used for anything imaginable, such as social networking, online shopping, online studying, online employment, and online jobs. In contrast to other forms of crime that occur in society, cybercrime is unique. It has no geographical boundaries, and no one knows who the cybercriminals are. All parties concerned, including the government, businesses, and people, are impacted by it. Cybercrime is on the rise in India as a result of the country's growing use of information and communication technologies. A few years ago, there was a lack of knowledge regarding the crimes that might be committed online, but today, India is not far behind other nations in terms of cybercrime, where the incidence of cybercrimes is also on the rise. According to the report of Norton Lifelock, a cybersecurity software company, in the last 12 months, 27 million Indian adults have been victims of identity theft, and 52 percent of people in the nation are unaware of how to defend themselves against cybercrime.This article was written to examine a brief introduction to cybercrime, its various types, and to analyse cybercrime in India. He goes on to highlight several measures to combat cybercrime in India.

KEY WORDS: **Cyber-crime, Technology, Internet, Communication.**

## INTRODUCTION

Internet has been the revolutionary invention of the 20th century. It successfully shrunk the world into a much smaller place by bringing the citizens and nations closer together in terms of enhanced communication and prompt exchange of ideas and information. Not only this, the internet has been the single most effectual device in spreading its existence without being restricted even by the international boundaries. Keeping aside its advantages, internet has also raised numerous security concerns which found place in highest levels of official and governmental discourses. Numerous untowardly instances like identity thefts, online frauds, breach of privacy, copyright infringement, financial theft, and cyber stalking accounted for a lack of trust among people.

The phrase "cybercrime" refers to any illegal conduct that makes use of computers or computer networks as a tool, a target, or a networked equipment. Examples include electronic theft and denial-of-service attacks. It is a catch-all term for crimes such as phishing, credit card fraud, bank robbery, illegal downloading, industrial espionage, child porn, kidnapping children through chat rooms, frauds, cyber terrorism, virus generation and/or dissemination, spam, and others. The majority of cybercrime is committed by cybercriminals or hackers

motivated by financial gain, although not all of it. While some cybercrimes directly target computers or devices in order to damage or disable them, others target computers or networks in order to distribute malware, unlawful content, offensive photos, or other items. Some cybercrime targets computers in order to spread a computer virus to other computers and, in some cases, entire networks.

It also includes traditional crimes where the criminal behaviour is enabled by computers or networks. Cybercrime is on the rise, and it's now acceptable to hack into other people's accounts for vengeance or to generate money by making bogus phone calls.

The Indian Legislature does not provide an exact definition of Cyber Crime in any statute, including the Information Technology Act of 2000, which deals with Cyber Crime. But, in general, cybercrime refers to any criminal conduct carried out via or with the assistance of the internet or computers.

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"

The oxford Dictionary defined the term Cyber Crime as "Criminal activities carried out by means of computers or the Internet."

Cyber Crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime"

## History of Cyber Crime

By 1820, the first cybercrime had been documented. The earliest known computers were built in Japan, China, and India around 3500 B.C., but Charles Babbage's analytical computer's current engine era is often thought of as the past.

A French manufacturer named Joseph-Marie Jacquard invented the loom in 1820. This apparatus enabled the weaving of complex materials in a continuous succession of processes. Since this new technology posed a direct danger to the jobs and income of the current Jacquard workforce, many of them resorted to sabotage in an effort to deter their employer from adopting it.

## TYPES OF CYBERCRIMES

Cybercrimes are classified into many sorts since they can be committed by targeting anything beneficial to a person or a nation. Let's examine each of these types individually.

### Identity theft

A criminal who gains access to a user's personal information can use it to steal money, gain access to sensitive information, or perpetrate tax or health insurance fraud. They can also use the person's name to get a phone/internet account, plan illegal actions, and apply for government benefits in your name. They could do so by stealing passwords from users, collecting personal information from social media, or sending phishing emails.

## I.Phishing

In such cases, hackers send malicious email attachments or URLs to users in order to get access to their accounts or computers. Because hackers are becoming more established, many of these emails are not flagged as spam. Users are tricked into clicking on links in emails that claim they need to reset their password or update their payment information, giving hackers access to their accounts.

### II.Social Engineering

Criminals utilise social engineering to contact you directly, usually via phone call or email. They usually pose as a customer service representative in order to gain your trust and collect the information they require. This information might include your passwords, the name of your company, or the number of your bank account. Before adding you as a friend on social media networks, cybercriminals will acquire as much information about you as possible on the internet. After gaining access to an account, they can sell your information or start accounts in your name.

## I. Cyberstalking

Cyberstalking is the practise of being followed by criminals on your social media accounts in order to get your private information and exploit it to their advantage. They have a variety of methods for gathering your information. They might be able to do this by intercepting user passwords, obtaining personal data through social media, or disseminating phishing emails. This form of behaviour includes, but is not limited to, threats, defamation, slander, sexual harassment, and other attempts to intimidate, control, or otherwise harm the victim.

## II.Botnets

Networks of compromised computers that are controlled remotely by hackers are known as botnets. Afterwards, remote hackers utilise these botnets to send spam or attack other computers. In addition to being used to carry out malicious actions, botnets can also act as malware.

## III.Prohibited content

In this type of cybercrime, cybercriminals distribute offensive and extremely disturbing content. Here, unpleasant and upsetting content includes films with violent content, unlawful videos, and videos about terrorism in addition to sexual content. This sort of data can be found on both the open internet and the dark web, an anonymous network.

### IV.Trojan attacks

The phrase "Trojan horse" is where this term first appeared in written English. This is a term used in the software industry to refer to an unapproved piece of software that secretly takes control of another person's computer by pretending to be an authorised piece of software. E-mail is the vector of choice when it comes to the propagation of Trojan horses. For example, a female film director in the United States had a Trojan horse virus installed on her computer while she was conversing online. The cyber criminal was able to collect nude images of the victim by using the web cam that was built into the computer. He continued to be harassing towards this lady.

### V.Web jacking

The phrase "hijacking" is where this term originated from. In these types of cybercrimes, the hacker acquires access to and control over the website that belongs to another person. It's possible that he'll even modify or delete some of the content on the website. This may be done with the purpose of satisfying political goals or for financial gain. For example, Pakistani hackers recently breached the security of the website for the Ministry of Information Technology, which resulted in the addition of explicit content to the website. In addition to this, the website of the Bombay crime branch was also taken over. The 'gold fish' case is an additional instance of web jacking that occurred. The material on the site referring to gold fish was altered once it was hacked in this particular instance. In addition, a ransom of one million dollars in United States currency was requested. In this sense, web jacking refers to the process of gaining control of the website of a third party in exchange for some form of benefit from that website

**REASONS FOR CYBER CRIME:**

Human beings are weak, hence the rule of law is necessary to safeguard them, according to Hart's statement in his book "The Idea of Law." Extending this to the internet, we may say that since computers are susceptible to cybercrime, the rule of law is necessary to keep them safe. Computers are vulnerable for the following reasons, in that order:

## I.The capacity for storing data on very little place

The computer has the remarkable ability to store information in a relatively limited amount of physical space. The fact that this enables one to extract or derive information using either a real or virtual media makes the process significantly simpler.

## II.Complexity

The operating systems are what allow the computers to function, and each operating system is made up of millions of individual codes. The human mind is flawed, hence it is impossible that there will never be an error in judgement at any point in time. In order to get into the computer system, the hackers take advantage of these gaps in security and do their best to sneak in.

### III.Negligence

The behaviour of humans is intricately linked to the concept of negligence. It is therefore highly conceivable that, while attempting to secure the computer system, there may be any neglect, which, in turn, creates an opportunity for a cyber criminal to acquire access to and control over the computer system.

## IV.Loss of evidence

Due to the fact that all of the data are frequently deleted, the loss of evidence is a very common and visible concern. The continued acquisition of data from beyond the territorial extent also renders this method of criminal investigation ineffective.

## V.Easy accessability

The challenge that arises when attempting to protect a computer system from unauthorised access is the fact that there is always the chance of a breach occurring not as a result of human error but rather as a consequence of the complicated technology. It is possible to get around many different security systems by using methods such as covertly implanted logic bombs, key loggers that can steal access codes, advanced voice recorders, retina imagers, and other similar devices that can trick biometric systems and circumvent firewalls.

## CYBER CRIMINALS:

The challenge that arises when attempting to protect a computer system from unauthorised access is the fact that there is always the chance of a breach occurring not as a result of human error but rather as a consequence of the complicated technology. It is possible to get around many different security systems by using methods such as covertly implanted logic bombs, key loggers that can steal access codes, advanced voice recorders, retina imagers, and other similar devices that can trick biometric systems and circumvent firewalls.

I. **Children and teenagers between the ages of 6 and 18 :**

The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reasons may be psychological even. E.g. the Bal Bharati (Delhi) case was the outcome of harassment of the delinquent by his friends.

II. **Groups of hackers working together:** These kind of hackers are typically part of a larger group that works together to achieve a specific goal. It's possible that they're doing it to satisfy their political bias, fundamentalism, or some other motivation.

III. **Professional hackers / crackers:** Their actions are influenced by the hue of the money. Hackers of this type are typically hired to penetrate the websites of competitors in order to obtain information that is trustworthy, dependable, and valuable. Also, they are hired by the employer to "crack the system," which is a euphemism for "finding the vulnerabilities in the system," as a step to make the system safer.

IV. **Discontented employees:** Those who fall into this category are either those that have been fired from their jobs or those who are unhappy with the work environment they currently occupy. They generally take revenge by hacking into the system of their employee**.**

## STATUTORY PROVISONS

The General Assembly of the United Nations accepted the Model Law on Internet Commerce that was adopted by the United Nations Committee on Trade Law, and the Indian parliament deemed it necessary to give effect to this decision so that it may become law. The Information Technology Act of 2000 was eventually approved and went into effect on May 17th, 2000 as a direct result of this. The goal of this Act is stated in the preamble, and it is to legalise online business transactions and make additional amendments to the Indian Evidence Act 1872, the Indian Penal Code 1860, the Banker's Book Evidence Act 1891, and the Reserve Bank of India Act 1934. Incorporating these amendments into these Acts is being done primarily for the aim of

making them consistent with the Act of 2000. So that they can more effectively regulate and manage the goings-on in the cyber realm.

## Conclusion

The human brain has an incredible processing capacity. No amount of effort will ever be enough to completely rid the internet of criminal activity. Certainly, it is possible to verify their authenticity. The annals of time bear witness to the fact that no legislation has ever succeeded in eradicating crime worldwide. Making people aware of their rights and duties (including the need to report crime as a communal duty towards society) and then applying the law more strictly are the only means by which crime can be reduced. Without a doubt, the Act is a watershed moment for the online community. However, I do not disagree that the Information Technology Act needs to be updated to better protect against cybercrime. In closing, I'd want to issue a word of warning to the pro-legislation camp, saying that it's important to keep in mind that overly stringent aspects of the cyber law could impede sector growth and prove counter-productive.

**References:**

1. Rashmi Saroha, "Profiling a Cyber Criminal", International Jour nal of Information and Computation Technology.Volume 4, Number 3 (2014).
2. http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 18 feb, 2023).
3. CYBER CRIME by Parthasarathi Pat, available at: https://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Accessed on 20th feb. 2023).
4. https://southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf
5. http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf
6. https://www.ijlmh.com/wp-content/uploads/Current-Scenario-of-Cyber-Crime-in-India.pdf