*LawPublicus*

The Legal Portal

Volume 1 : Issue 1

Maiden Issue

November 2020

Email ID: Lawpublicusportal@gmail.com

Website: www.Lawpublicus.com

# Disclaimer

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of ***LawPublicus*** The Legal Portal. The Editorial Team of ***LawPublicus*** holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of ***LawPublicus***. Though all efforts are made to ensure the accuracy and correctness of the information published, ***LawPublicus*** shall not be responsible for any errors caused due to oversight or otherwise.

FOR *LawPublicus* The Legal Portal

# Editorial Team

# About Us

***LawPublicus*** The Legal Portal is a leading journal of multidisciplinary research. It is a free, peer-reviewed, open-access journal that provides insight into diverse and dynamic legal matters.

***LawPublicus*** is a novel initiative by legal minds. As the its name suggests, it is platform for young minds to ignite their willingness and inventiveness in order to contribute to the field of law through new ideas, opinions and thereby contributing to an informed citizenry.

We hope to provide a forum for young and enthusiastic writers to voice their feelings and research on interdisciplinary approaches. We also have in view to evaluate, explore and deliberate, under the tutelage of seasoned editors and academic experts, on current trends and projections based thereon in legal studies. LawPublicus focuses not only on the scholarly writings but also on numerous other approaches such as discussions, interviews, and debates with experts and qualified & industrial professionals.

We are determined and excited to bring authentic, creative and individual ideas and socially-related problems into attention.

***LawPublicus*** calls for research papers, articles, short notes, book reviews & case commentaries, that are distinctive and unpublished.

With this thought, we hereby present to you

*LawPublicus* The Legal Portal

# CYBER CRIME(S) AND CYBER SECURITY: A DETAILED ANALYSIS

**AUTHORED BY:**

***YASHWANTH A S***
***CHFI; CEH***
**Contact: +91-9591546911**
**Email ID: as.yashwanth@gmail.com**

# CYBER CRIME(S) AND CYBER SECURITY: A DETAILED ANALYSIS

***By: YASHWANTH A S***

## ABSTRACT:

In India each and every minute one person becomes an internet user. Its convergence with digitally supported platforms and gadgets, safeguarding the oldsters moreover as students from the cybercrimes is becoming a challenging task. Additionally, the pinching reality is that the web users aren't getting updated on the vulnerable cyber threats and security issues, at the pace they're getting updated with the usage of internet enabled tools and apps. Thus the present research paper focuses to find out the answers to alarming questions – "Is the citizens really aware that they're at risk of various Cybercrimes?" "If they're aware, to what extent?", "If common people are not very conscious about cyber-crimes, what measures have to be adopted to create an awareness to the citizens and updated day to day life. The paper suggested a conceptual model explaining a way to uphold and implement the notice programmes among internet users regarding cyber-crimes. People's dependence and behaviour towards information security and the internet deeply affect the way they will use information technology.

The increased dependence of individuals on the internet has led to the increase in cybercrime. There are problems like, no proper training has been given and also in education, the poor of cybercrime awareness among Indians have also contributed to cybercrime. Even the enforcement has faced huge problems in tackling cyber-crimes because of the high rate of cybercrime. The paper intends to grasp the notice level of cybercrime among various college students of Kochi. The paper also intends to seek out the faculty students' awareness on the kinds of cybercrimes and also the various government schemes.

## INTRODUCTION:

Cyber law in India needs such laws in order that people can perform purchase transactions over the online through credit cards without concern of misuse. The Act offers the much-needed legal framework so information isn't denied legal effect, validity or enforceability, solely on the bottom that it's within the type of electronic records. Cybercrime is inescapable, ubiquitous and increasingly linked with different parts and areas of criminal environs. This evolution and network gave rise to cyberspace which controls and manages to produce equal opportunities and facilities to all or any people to access any reasonable information. Thanks to the gradual increase of the web, abuse of technology is broadening gradually which tends to cybercrimes. Cybercrime is essentially an unlawful act that ends up in criminal activity.

Cyber Security, a mechanism by which pc information and also the equipment's are protected against unauthorized and illegal access.

Nowadays Computer crime issues and thefts have become tremendously high-profile, particularly those surrounding violation, hacking, erotica, child grooming, and spoofing. These days' computers and the internet have become very Necessary and useful for our standard of living. Today the web is the great mediator of our lives. In present days people can get information, store information and share information through the web.

Today the cyber world is the fastest moving and engineering world. Asian countries have the most uses of the internet within the world. In Asia region India has ranked in the top two internet users country, so India is that the very fastest growing country. The Internet has become the backbone today in the everyday socio economic world. Users can access the web anytime from anywhere but through the net many illegal works can be done.

Today Email and websites are the best way of information communication. India is trying to implement the Digital India project to the most effective of its capabilities. The success of Digital India project would rely upon maximum connectivity with minimum cyber security risks.

## **CYBER CRIMES / CYBER FRAUDS:**

Cybercrime is the latest and maybe the foremost complicated problem for the cyber world. In India, law has not given any particular definition for the term 'cybercrime'. In fact, the Indian legal code doesn't use the term 'cybercrime' at any point even after its amendment by the knowledge Technology (amendment) Act 2008, the Indian Cyber law. "Cyber terrorism is that the premeditated, politically motivated attack against information, computer systems, computer programs, and data which lead to violence against property, government and other people at large. Or by “Acts which are punishable by the Information Technology Act”.

In India, Information Technology Act, 2000 deals with the cybercrime problems.it covers following areas commercial transactions online, use digital signatures defined various cybercrimes, electronic commerce.

**Cyber Crimes Includes:**

- E mail Bombing: this can be a heavy crime during which someone sends a number of emails to the inbox of the target system/person. Mail bombs will usually fill the allotted space on an e-mail server for the users email and may end in crashing the email server.

- Hacking: among all kinds of cybercrime it's the foremost dangerous and serious threat to the net and e-commerce. Hacking simply refers to the breaking into the pc system and steals valuable information (data) from the system with none permission. Hacking is completed by hackers now the question arises who are hackers; hackers are in b/w client & server and able to spoof the data/info. Duplication the IP address illegally.

- Spreading Computer Virus: It's a group of instructions which is ready to perform some malicious operations. Viruses stop the traditional function of the system programs and also to the full system. They'll also ruin/mess up your system and render it unusable without reinstallation of the software package. A computer virus is spread through Emails, CDs, Pen drives (secondary storage), Multimedia, and Internet.

- Phishing: It simply refers to stealing information like passwords, master card details, usernames etc. over the web. Phishing is usually allotted by email spoofing and instant messaging. During this kind of crime hackers make a right away link which directs to the fake page /website which looks and wants just like the legitimate one.

- Identity Theft: It simply refers to fraud or cheating others by making their wrong identity of others. It involves stealing money or getting other benefits by pretending to somebody else Information Technology (Amendment)Act, 2008, crime of fraud under Section 66-C. Whoever, fraudulently or dishonestly make use of the electronic signature, password or the other unique identification feature of the other person, referred to as fraud that criminal shall be punished with imprisonment of either description for a term which can touch three years and shall even be susceptible to fine which can reach rupees one lakh.

- Internet Fraud: Internet fraud can occur in chat rooms, email, message boards or on websites. In internet fraud, criminals can send fake info to the victim in cases like online purchasing, property, pay BAL, Work-at-home donation processing etc.

- Malicious Software: These are Internet-based software or programs that are accustomed to disrupt a network. The software is employed to realize access to a system to steal sensitive information or data or causing damage to software present within the system.

- Cyber Warfare: It's an Internet-based conflict involving politically motivated attacks on information systems. Cyber warfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems -- among many other possibilities.

- Domain Hijacking: It's the act of adjusting the registration of a site name without the permission of its original registrant.

- SMS Spoofing: SMS Spoofing allows changing the name or number text messages appear to return from.

- Voice Phishing: The term may be a combination of "voice" and phishing. Voice phishing is used to achieve access of personal, personal and financial information from the general public. Voice phishing uses a landline telephone to urge information.

- Cyber Trafficking: It's going to be trafficking in weapons, drugs, kinsmen, which affect the big numbers of persons.

## INFORMATION TECHNOLOGY ACT, 2000:

India, has been enforced the Information Technology Act in the year 2000 which deals with the cybercrime activities or the issues. It act 2000 has both positive and negative aspects similarly. Therefore amendment is completed in Rajya Sabha on Dec 23rd of 2008.this act was renamed as Information Technology (Amendment) Act, 2008 and referred as ITAA 2008. is that the new trick and Methodology of concept using computer and internet to retrieve, transmit, store, update, manipulate, and delete computer data or information, often within the context of business or other enterprises IT body.

The technology mainly growing in the 21st century was a technological revolution which encompassed not only India but the whole world. The utilization of computers isn't limited to established institutions or organizations, but available to each individual at the swipe of a finger. It's eased out almost every humanized action. The unparalleled use of the internet in our day-to-day lives also led to commencement of misuse of the internet like data theft, illegal personal, and interference with privacy, cybercrimes etc.

Computer fraud may be an untrustworthy misrepresentation of the actual fact proposed to prompt another to abstain from doing something that causes loss. Computer crime will be summarized as a criminal activity which involves information technology infrastructure, additionally to unauthorized access, illegal interception, any data interference, computer or systems interference, abusage of devices, forgery, blackmail, embezzlement, and a few electronic frauds.

There exits privacy issues whenever any hint or data is hijacked or lost, either lawfully or otherwise. Cybercrime cells are there in states basically to handle these crimes, and to expel or punish the netizens or criminals committing any of the cybercrime. It basically ranges from theft of an individual’s identity to the entire disruption of a specific country’s Internet and network connectivity thanks to massive attacks across its networking resources. During this digital age, online communication now becomes a norm, the net users and therefore the government are at an enlarged risk of becoming the bull's-eye of cyber-attacks. Cybercrime can cause harm to any organization Hacking of the ATM password, transferring the cash by hacking the checking account details of the victim's account to theirs, some pornography issues etc. are a number of the thefts that are handled by educated people. There's an urge to implement a number of the foundations and regulations, to tackle and handle these crimes governing cyber space particularly called Cyber Law.

## ELECTRONIC CONTRACTS:

It has been in force from17th May 2000 and amended further as the Information Technology (Amendment) Act, 2008 which was enforced on 27th October 2009. In India, cyber laws are contained within the Information Technology Act, 2000 ("IT Act") which came into force on October 17, 2000. The data technology amendment act 2008 has been passed along the parliament on 23rd December 2008. It received the assent of the president of India on 5th February 2009.

The main purpose of the Act is to produce legal recognition to electronic commerce and to facilitate filing of electronic records with the government Information Technology Act, 2000 is India’s mother legislation regulating these of computers, computer systems and computer networks as also data and data within the electronic format.

The IT Act 2000 attempts to alter outdated laws and provides ways to house cybercrimes as from the potential of E-Commerce in India, IT act 2000 contains many positive aspects like companies shall now be ready to perform E-Commerce using Legal Infrastructure for the authentication and origin of transmission through digital signatures. But it's considered to be the ambiguous law within the area of jurisdiction within the context of the net. As sec 1 (2) provides that the act shall extend to the full of India and save as otherwise provided during this Act, it applies also to any offence or contravention there under committed outside India by someone. Similarly, sec 75 (2) provides that this act shall apply to an offence or contravention committed outside India by someone if the act or conduct constituting the offence or contravention involves computer, automatic data processing system or network located in India.

This type of provision appears to be against the principle of justice. In fact, the term ‘cybercrime’ at any point even after the amendment by the IT Act Amendment 2008. They have to push the cyber laws. The Data Technology Act is an outcome of the resolution dated 30th January 1997 of the final Assembly of the global organization, which adopted the Model Law on E-Commerce, which is adopted as the Model Law on E-Commerce on International Trade Law. Cyber law is very important because it touches most aspects of transactions and activities on and involving the web, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives.

## CYBER LAW ENCOMPASSES LAWS RELATING TO:

Cyber-crimes:

- Electronic and digital signatures
- Intellectual property
- Data protection and privacy.
- To provide legal recognition for transactions:-
- Carried out by means of electronic data interchange, and other means of transmission, commonly noted as "electronic commerce“
- To facilitate electronic filing of documents with Government agencies and E-Payments
- To amend the Indian legal code, Indian Evidence Act,1872, the Banker's Books Evidence Act 1891, Reserve Bank of India Act ,1934
- Computer crimes within the Act are classified into two categories:
- Civil offences
- Criminal offences

## SALIENT FEATURES OF THE KNOWLEDGE TECHNOLOGY (AMENDMENT) ACT, 2008:

The term 'digital signature' has been replaced with 'electronic signature' to form the Act more technology neutral. a replacement section has been inserted to define 'communication device' to mean cell phones, personal digital assistance or combination of both or the other device wont to communicate, send or transmit any text video, audio or image. A replacement section has been added to define cyber cafe as any facility from where the access to the net is obtainable by anyone within the ordinary course of business to the members of the general public. New Section to deal with data protection and privacy -Section 43 Body corporate to implement best security practices-Sections 43A &72A

## IT (AMENDMENT) ACT, 2008:

- IT act 2008 could be a re-creation of IT act 2000.
- Provides additional concentrate on information security.
- Added several new sections on offences including cyber terrorism and data protection.
- 124 sections and 14th chapters.
- Schedule 1 and a couple of are replaced and scheduled 3 and 4 are deleted.

**IMPORTANCE OF CYBER LAW:**

• We reside in a highly digitalized world.

• All companies depend on their computer networks and keep their valuable data in electronic form.

• Government forms including tax returns, company law forms etc. are now filled in electronic form.

• These days, consumers are using more and more credit and debit cards for online shopping and offline like in supermarkets also.

• Most people are using email, cell phones and SMS messages for communication.

• Even in non-cybercrime cases important evidence is found in computers/ cell phones e.g. in cases of divorce murder, kidnapping, social group terrorist operations counterfeit curacy etc.

• Cyber Law is extremely important because of the aspects of transaction and activities on the web, the globe Wide Web and cyberspace therefore.

## CYBER LAWS IN INDIA:

The 20th century introduced new requisites and offenses to the law glossary. Legal provisions should provide assertion to users, enforcement agencies and deterrence to criminals because it is incredibly important to grasp that computers cannot commit against the law but act on individuals. It's the personalities, not machines, who abuse, demolish and warp information. By realizing the requirement to combat with the cyber violations, the UNCITRAL, i.e. the world organization Commission on International Trade Law adopted the Model Law of Electronic Commerce in 1996.

It was followed by the final Assembly of United Nations recommending that everyone states should give favourable considerations to the State Model law. In discharge of its responsibility, Government of India also accepted the requirement to legislate and has approached the new legislation Information Technology Act, 2000. It had been amplified by its amendments. the key acts, which got amended after enactment Information Technology Act , are Indian legal code ( e.g. 192, 204 ,463, 464 , 468 to 470 , 471 , 474 , 476 etc. ) before enactment of IT Act , all evidences in a very court were within the physical form only after existence of IT Act , the electronic records and documents were recognized.

## THE ACT ESSENTIALLY DEALS WITH THE SUBSEQUENT ISSUES:

- Legal identification of Electronic documents.
- Legal identification of Digital Signatures
- Offenses and Contraventions Justice
- Dispensation Systems for cybercrimes.

## NEED FOR CYBER LAW:

- The Internet has dramatically changed our life.
- Transaction from paper to paperless world.
- Laws of the universe cannot be interpreted within the light of emergency cyber space.
- The Internet requires an enabling and supportive legal infrastructure to tune with the days.

Cyber law is the law governing cyberspace.
Cyberspace includes computer networks software, data storage devices (such as hard disks, USB, disks and internet websites, emails, and even electronic devices like cellophanes ATMs, machines, etc.

## CATEGORIES OF CYBERCRIME:

3 category of cyber-crimes -

a. Cyber Crimes against person.

b. Cybercrime against property.

c. Cybercrimes against the government.

## APPLICABILITY:

### Digital Signature under the IT Act, 2000:

Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3. Electronic Signature:-Electronic signature has also been treated under Section 3A of the IT Act, 2000. A subscriber can authenticate any electronic record by such electronic signature or electronic authentication technique which is taken into account reliably and should be per the Second Schedule. An Amendment to the IT Act in 2008 introduced the term electronic signatures. The implication of this Amendment is that it's helped to broaden the scope of the

IT Act to incorporate new techniques as and when technology becomes available for signing electronic records aside from Digital Signatures.

E-Governance:-E-governance or Electronic Governance is forbidden under Sections 4 to 10A of the IT Act, 2000.

It provides for legal recognition of electronic records and Electronic signature and also provides for legal recognition of contracts formed through electronic means. Filling out of any form, an application or any other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or the payment to be made Government offices and its agencies could also be done through the means of electronic form.

## SOME IMPORTANT SECTIONS OF IT ACT 2000:

- Cyber Stalking: Stealthy following a person, tracking his Internet chats. Sections are 43, 65 and 66 of the IT Act, 2000. Punishment is up to 3 years imprisonment and/or fine up to Rs 2 Lakh.
- Cyber Pornography including Child Pornography: Publishing Obscene in Electronic Form involving children. Section 67 and 67(2) of the IT Act, 2000. Punishment is 10 years imprisonment and/or with fine may extend to 10 lakh.
- Intellectual Property Crimes: Source Code Tampering, piracy, copyright infringement etc. Section 65 of the IT Act, 2000. Punishment is 3 years imprisonment or with fine up to 2 lakh
- Cyber Terrorism: Protection against cyber terrorism. Section 69 of the IT Act, 2000. Punishment is 10 years imprisonment and with fine may extends to 10 lakh
- Cyber Hacking: Destruction, deletion, alteration, etc. in computer resources. Section 66 of the IT Act, 2000. Imprisonment is 3 years imprisonment or fine up to 2 lakh.
- Phishing: Bank and Financial Frauds in Electronic Banking. Sections 43, 65 and 66 of the IT Act, 2000. Punishment is 3 years imprisonment or with fine up to 2 lakh.
- Privacy: Unauthorized access to computers. Sections 43, 66, 67, 69 and 72 of the IT Act, 2000. Punishment is 2 years imprisonment or with fine up to 1 lakh.

## IMPACT OF CYBER CRIME:

Worms are the foremost strong style of cyber-attack which causes severe disruption. Within the month of September, in 2010, Stuxnet infected and affected the unknown number of business controls round the whole world, and stealthily gave invalid instructions to the machinery and a few false readings to the operators. Potentially, it destroys gas pipelines, causes nuclear plants to malfunction or causes boilers of factories to explode. This worm was known to move mostly in Iran, on the identical Indonesia, Pakistan, India also reported as infections.

Crime against People during this, the criminal provides numerous false promotions and offers the people an illusion of security by forcing them to administer their personal information. It includes smut, a dominant offence. Social networking sites and also the discussion groups also can be concluded as a heavy cybercrime from time to time.

Crime against Property Criminals can easily with their techniques steal the private information of the opposite people ADP system and therefore the theft gains the unauthorized access to an online connection, is a cybercrime.

Crime against Business during this crime, criminals basically hack the system or machine of any business organization; they store and steal the confidential and also the sensitive data of the system on the server.

They acquire unauthorized access to the secured and confidential data of the corporate and via this, they transfer funds of the corporate to their accounts that produces the organization bankrupt. Crime against Government Cyber terrorism could be a term used against government crime during which hackers hacks the secured and confidential database of the government with the urge to use sensitive and private information of the govt. that reduces the religion of the citizens.

## **TYPES OF HACKERS:**

Any criminals or hackers are usually engineers, doctors, Non-technical students etc. all educated folks that try to realize the access of other systems. These are three kinds of hacker. White Hat Hackers they're ethical hackers who basically specialize in securing and protecting IT systems. White hat hackers are people who attempt to interrupt a network or system so as to assist the holder of the system by making an attempt to aware them of the protection flaws. Many such quite people are employed by the businesses concerning about the PC security;

these are professional sneakers and also the collective group of them are often categorized as tiger teams. Black Hat Hackers a private who compromises with the protection of computing system with none

Acknowledgement from the authorized party. They use their knowledge to take advantage of the systems. Grey Hat Hackers A grey Hat Hacker is taken into account as a talented hacker within the security community who sometimes acts legally, and sometimes not. They're considered a hybrid between black and white hat hackers. They basically don't hack with the malicious intentions.

## **CYBER SECURITY:**

A branch of technology basically referred to as cyber security or information security applied to networks and computers, the target carries protection of knowledge or information and therefore the property from the thefts, natural disaster, or corruption, and allowing the property and knowledge to stay productive and accessible to its users .The Cyber security implies to the processes and therefore the technologies which are designed to guard networks, computers and therefore the data from the unauthorized access, attacks, and vulnerabilities delivered via the net by cyber criminals. Cyber security requires global co-operation to house the protection of cyberspace. It protects computer Equipment, resources of computers or systems, information and data from any unauthorized access and also the disclosure.

During this paper different sorts of attacks and threats are overviewed. Each and each attack is described firmly, and categories of hackers also are reviewed.

In section II, cybercrime is detailed together with its two classifications of sorts of crimes.
In section III differing types of attacks are briefly overviewed.
Section IV, category of hackers is acknowledged.
Section V cyber crime’s impact is detailed.
Section VI, there’s a brief overview of cyber security is organized.

## CYBERCRIME PREVENTION STRATEGIES:

Newer versions of Cybercrime is taken into account one the foremost dangerous threats for the event of any state; it's a heavy impact on every aspect of the expansion of a rustic. Cyber-criminal syndicate includes several institutions like Government entities, NGO's, private companies and citizens all potential has been targeted.

Cyber criminals are not any different than traditional criminals therein they require to create their money as quickly and simply as possible. Cybercrime prevention may be achieved fairly quickly and during a cost-effective manner.

The prevention of cyber-criminal activities is the most crucial aspect within the fight against cybercrime. It mainly supported the concepts of awareness and data sharing.

A correct security posture is the best defence against cybercrime. Every single user of technology must bear in mind of the risks of exposure to cyber threats, and will be educated about the simplest practices to adopt so as to scale back their "attack surface" and mitigate the risks.

## NATIONAL CYBER SECURITY POLICY STRATEGIES:

- Creating a secure cyber ecosystem.
- Creating an assurance framework.
- Encouraging Open Standards.
- Strengthening the Regulatory framework.
- Creating a mechanism early warning for security threat, vulnerability management and speedy response to the security threats.
- Securing E-Governance services.
- Protection and resilience of Critical Information Infrastructure.
- Promotion of Research & Development in cyber security.
- Reducing supply chain risks.
- Human Resource Development.
- Creating Cyber Security Awareness.
- Developing effective Public Private Partnership.

- Information sharing and cooperation.
- Prioritized approach for implementation.

## MANAGEMENT OF CYBER SECURITY RISKS:

- Threats (attacking by whom and to what extent has been attacked),
- Vulnerabilities (the weaknesses they're targeting upon),
- Impacts (what are the results of the attack).

The management of risk is taken into account fundamental to effective cyber security. What are the Threats? People who actually or potentially perform cyber-attack are widely cited to be one or more of 5 categories:

- Criminal's bent on monetary gain from crimes like theft or extortion.
- Spies bent on stealing classified or proprietary information employed by government or private entities.
- Nation-state warriors who develop capabilities and undertake cyber-attacks in support of a country's strategic objectives.
- "Hacktivists" who perform cyber-attacks for nonmonetary reasons.
- Terrorists who engage in cyber-attacks as a sort of non-state or state-sponsored warfare.

## WHAT ARE THE VULNERABILITIES?

Cyber security is in many ways a race between attackers and defenders. ICT systems are very complex, and attackers are constantly craving for weaknesses, which may occur at many points. Defenders can protect often against weaknesses, but three are particularly challenging: inadvertent or intentional acts by insiders with access to a system.

Supply chain vulnerabilities, which might permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or zero-day, vulnerabilities with no established fix.

Even for vulnerabilities where remedies are known, they'll not be implemented in many cases thanks to budgetary or operational constraints.

## WHAT ARE THE IMPACTS?

A successful attack can compromise the confidentiality, integrity, and availability of an IT system and also the information it handles. Cyber theft or cyber espionage may result in exfiltration of monetary, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. Denial-of-service attacks can slow or prevent legitimate users from accessing a system. Botnet malware can give an attacker command of a system to be used in Cyber-attacks on other systems.

Attacks on industrial control systems may result within the destruction or disruption of the equipment they control, like generators, pumps, and centrifuges. Online games which misguide the online or cell-phone users also are samples of cybercrimes. The results of such games could also be as harmful as committing suicide by the player or theft of secret credentials from the players' digital devices.

## CONCLUSION:

In this modern technology of Indian cyber law, the role and usage of the internet is increasing worldwide rapidly, therefore it becomes easy for cyber criminals to access any data and data with the assistance of their knowledge and their expertise. Cybercrime is an unlawful act or a menace that must be tackled firmly and effectively.

Security nowadays is becoming a prominent and major concern. Within the following paper, some IT Law & security issues are introduced, threats, Trojans, and attacks over the internet. Computer security becomes critical in many of the technology-driven industries which operate the pc systems. Computer security is nothing over computer safety. Countless vulnerabilities and computer or network based issues act as an integral part of maintaining an operational industry. Despite being world-known as an information technology superpower, India lags far behind when it involves official cyber security workforce which comprises a little number of experts deployed in various govt agencies. Cyber security is becoming an imperative dimension of data security. It is often concluded from this present study that with increasing rate of cybercrimes more detection techniques together with educating the users on being safe online has to be established with complete guidance to grasp about the pros and cons of the online before entering it. One among the most important security concerns today is that the insider threat.

Another major security concern is lack of consistency in enforcing “acceptable use” policy. Concrete measures must be found so as to trace electronics evidence and preserve them in order that systems are better protected against cyber intrusions. To defend against cybercrimes, intrusion detection techniques should be designed, implemented, and administered. The thanks to protect it for now's for everybody to be smart and to follow preventive measures. Individuals, institutions, and governments should all follow these measures. It's time that the countries of the planet, including India, realise that a well-protected cyberspace would only be an asset to developing and developed nations.

In view of the rapidly growing threats to national security in cyberspace there's urgent need for the governments to adopt well developed cyber security policies. Cyber security education, R&D and training should be an integral part of the national cyber security strategy.

India is progressing during this area by implementing proper policies and by implementing simple laws. The state yet as national governments are taking steps to forestall cybercrimes but the efforts haven't been enough thus far. There's still a requirement of developing a talented and experienced task force. We would like to expedite our efforts during this field because the threats of cybercrimes and cyber war are increasing exponentially day by day.

---

*This article is for information purpose only. Nothing contained herein shall be deemed or interpreted as providing legal or investment advice.*