Cyber Law in India

By Viral Parmar

The Hackers Meetup™
Let's Talk About Hacking

Who Am I

@viralparmarhack

Viral Parmar

ComExpo Cyber Security Foundation
Cyber Security Researcher
Mozilla Reps, Mozilla Foundation
Given 700+ session all over the world
Solved 500+case of cyber crime and aware more then 10 lakh people about privacy and security
Motto: Know hAckiNG, but no HaCKing.

COMEXPO CYBER SECURITY FOUNDATION

Recent Cyber Crime Trends

The Ministry of Electronics and Information Technology said proactive tracking by CERT-In and improved cyber security awareness among individuals and organisations across sectors has led to increased reporting of incidents, that Indian citizens, commercial and legal entities faced almost 7 lakh cyber attacks till August 2020.

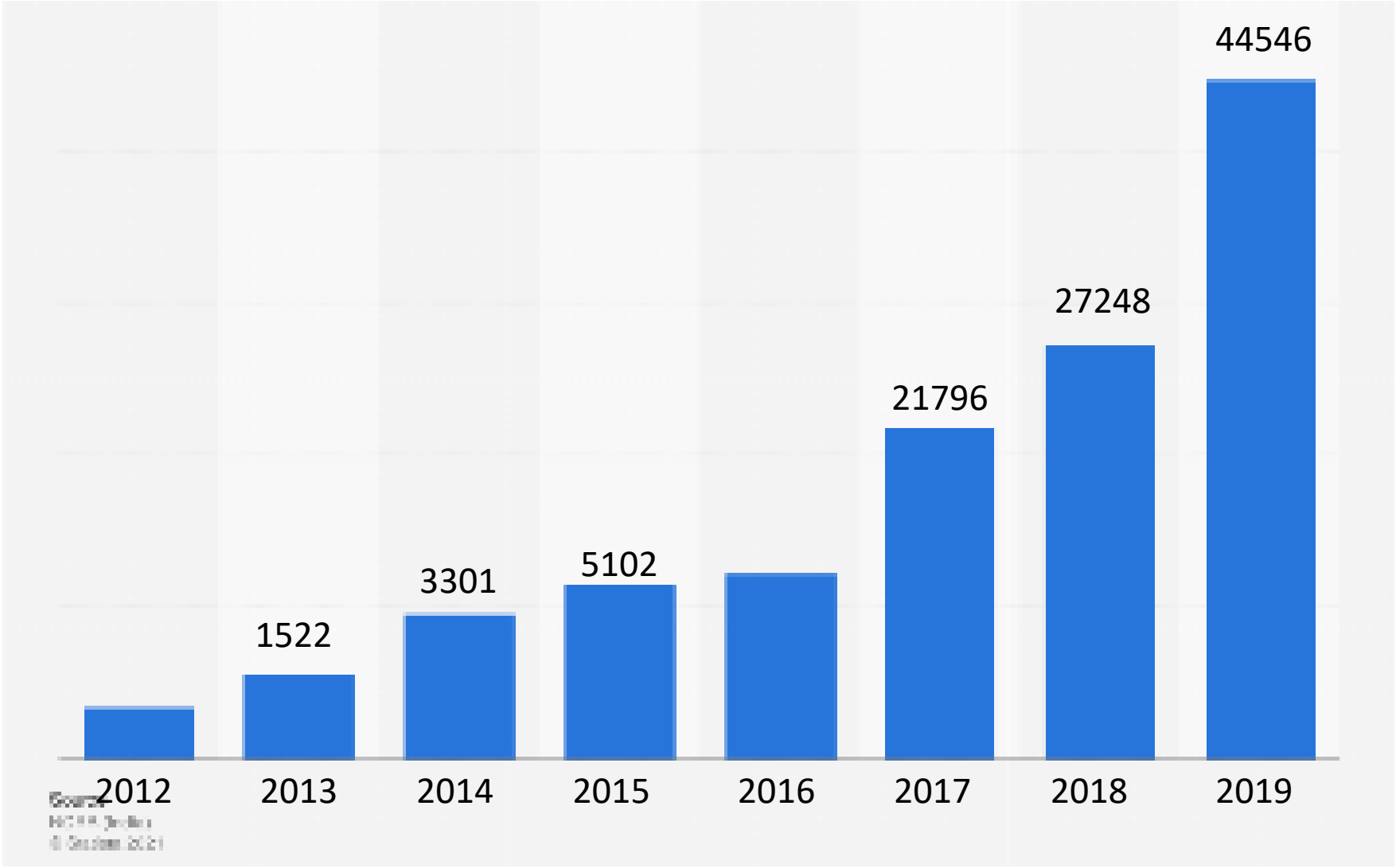
The Indian Computer Emergency Response Team (CERT-In) has “reported 49,455, 50,362, 53,117, 208,456, 394,499 and 696,938 cyber security incidents during the year 2015, 2016, 2017, 2018, 2019 and 2020 (till August) respectively”

As per the data from Computer Emergency Response Team (CERT-In) shows cyber attacks amid the Covid-19 pandemic rose by almost 300% last year in the country to reach 1,158,208 compared to 394,499 in 2019.

Since September 2019 3,17,439 cybercrime incidents and 5,771 FIRs have been registered up to February 28, 2021 in the country which includes, 21,562 cybercrime incidents and 87 FIRs in Karnataka and 50,806 cybercrime incidents and 534 FIRs in Maharashtra.

Over 2.9 lakh cyber security incidents related to digital banking were reported in 2020, As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total number of 1,59,761; 2,46,514 and 2,90,445 cyber security incidents pertaining to digital banking were reported during 2018, 2019 and 2020, respectively, These incidents included phishing attacks, network scanning and probing, viruses and website hacking.

Increase of Cyber Crime in India



Cyber Crimes Cases in 2019

Sno.	State	Cyber crime in 2019	Percentage Share of State
1	Karnatak	12020	27
2	Uttar Pradesh	11416	25.6
3	Maharashtra	4967	11.2
4	Telangana	2691	6.0
5	Assam	2231	5.0
6	Gujarat	784	1.8

Motives behind cyber crime

Motive	No. of cyber crime
Personal Revenge	1207
Anger	581
Fraud	26891
Extortion	1842
Causing Disrepute	1874
Prank	588
Sexual Exploitation	2266
Political Motives	316
Terrorist Activites	199

Motive	No. of cyber crime
Hate against Country	49
Disrupt Public Services	28
Sales/purchase of Drugs	10
Developing Own Business	181
Spreading Piracy	45
Steal Information	93
Other	7578

Who Did That

Profile of person	No of Crime
Employee Disgruntled	249
Neighbour/Relative	1195
Sexual Freak	415
Student	814
Professional hacker	1095

What is Cyber Crime?

Creates high Impact: Impact is severe and may be for long term

- Targeted Cyber crime
- Computer as a tool
  Stolen data, piracy , online hacking , bank fraud, website hacking
- Mobile as a tool - Storage device for digital evidence, (sms)hing, threat, sexual harassment, free calls(VOIP), mobile theft cloning
- Any electronic device

Types of Cyber Crime

- Hacking (Under Section 66 ITAA 2008)
- Denial of Service (DoS) (DDoS) attack (Under Section 66 of ITAA 2008)
- Spreading viruses and malware (Under Section 66 of ITAA,2008)
- Website defacement (Under Section 66 of ITAA 2008)
- Cyber terrorism (Under Section 66F of ITAA 2008)
- Spoofing (Under Section 66A, 66D of ITAA 2008)
- Skimming (Under Section 66C of ITAA 2008)
- Pharming /click frauds/ fake links (Under Section 66C, 66D of ITAA 2008)
- Spamming (Under Section 66A of ITAA 2008)
- Social engineering
- Phishing/vishing
- Password cracking
- Scam – charity , lottery, share

Types of Cyber Crime

- Banking/Financial fraud

(Several sections under IPC, ITAA 2008 and other applicable laws)

- Data modification

(Under Section 66 of ITAA 2008 and sections 403,406,408,409 of IPC as applicable)

- Identity theft and its misuse

(Under Section 66C, 66D of ITAA 2008)

- Cyber bullying/Stalking

(Under Section 66A of ITAA 2008 and sections 500,504,506,507,508,509 of IPC as applicable)

- Data theft

(Under Section 66 of ITAA 2008 and section 379 IPC)

- Pornography

(Under Section66E, 67, 67A and 67 B of ITAA 2008 and section 292 IPC)

- Theft of trade secrets and intellectual property

(Under Section 66 of ITAA 2008, IPR laws and other applicable laws

- Espionage on protected systems

(Under Sections 66, 70 of ITAA 2008 and other applicable laws)

Techniques of Cyber Crime

- Buffer overflow
- Cracking
- Data Didling
- Malware
- Ransomware
- Phishing
- Salami Attack
- Sniffer
- Social Engineering
- Spoofing
- Steganography
- Identity Theft
- DoS/Ddos
- APT
- Brute force / Password Cracking
- Wifi Hacking
- Mobile Hacking
- Exploit
- Spam

CYBERSPACE & REQUIREMENT OF CYBER LAWS

Cyber Law

43. [Penalty and compensation] for damage to computer, computer system, etc.–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,–

(a) accesses or secures access to such computer, computer system or computer network [or computer resource];

(*b*) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(*c*) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(*d*) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

Cyber Law

(*e*) disrupts or causes disruption of any computer, computer system or computer network;
(*f*) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
(*g*) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
(*h*) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
1[(*i*) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
(*j*) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]
2[he shall be liable to pay damages by way of compensation to the person so affected.]

Cyber Law

[43A. Compensation for failure to protect data.–Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Cyber Law

65. Tampering with computer source documents.–Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
Explanation.–For the purposes of this section, ―computer source code‖ means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Cyber Law

66. Computer related offences.–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

66A. Punishment for sending offensive messages through communication service, etc.–Any person who sends, by means of a computer resource or a communication device,–
(*a*) any information that is grossly offensive or has menacing character; or
(*b*) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;
(*c*) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

Cyber Law

66B. Punishment for dishonestly receiving stolen computer resource or communication device.–Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

66C. Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

66D. Punishment for cheating by personation by using computer resource.–Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Cyber Law

66E. Punishment for violation of privacy.–Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

66F. Punishment for cyber terrorism.–(*1*) Whoever,–
(*A*) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by–
(*i*) denying or cause the denial of access to any person authorised to access computer resource; or
(*ii*) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
(*iii*) introducing or causing to introduce any computer contaminant,
and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

Cyber Law

(*B*) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, 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,

commits the offence of cyber terrorism.

(*2*) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Cyber Law

67. Punishment for publishing or transmitting obscene material in electronic form.–Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.–Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Cyber Law

67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.–Whoever,–
(*a*) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
(*b*) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or 26
(*c*) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
(*d*) facilitates abusing children online, or
(*e*) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Cyber Law

67C. Preservation and retention of information by intermediaries.–(*1*) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
(*2*) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (*1*) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.]

68. Power of Controller to give directions.–(*1*) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.
[1][(*2*) Any person who intentionally or knowingly fails to comply with any order under sub-section (*1*) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or a fine not exceeding one lakh rupees or with both.]

Cyber Law

69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.–(*1*) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (*2*), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

Cyber Law

69A. Power to issue directions for blocking for public access of any information through any computer resource.–(*1*) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (*2*), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(*2*) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(*3*) The intermediary who fails to comply with the direction issued under sub-section (*1*) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

Cyber Law

69B. Power to authorise to monitor and collect traffic data or information through any computer resource for cyber security.–(*1*) The Central Government may, to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country, by notification in the Official Gazette, authorise any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

(*2*) The intermediary or any person in-charge or the computer resource shall, when called upon by the agency which has been authorised under sub-section (*1*), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.

(*3*) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(*4*) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (*2*) shall be punished with an imprisonment for a term which any extend to three years and shall also be liable to fine.

Cyber Law

70. Protected system.—[1][(*1*) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.

Explanation.–For the purposes of this section, ―Critical Information Infrastructure‖ means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.]

(*2*) The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section (*1*).

(*3*) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

[2][(*4*) The Central Government shall prescribe the information security practices and procedures for such protected system.]

Cyber Law

72. Penalty for Breach of confidentiality and privacy.–Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72A. Punishment for disclosure of information in breach of lawful contract.–Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.]

Cyber Law

75. Act to apply for offence or contravention committed outside India.–(*1*) Subject to the provisions of sub-section (*2*), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
(*2*) For the purposes of sub-section (*1*), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

80. Power of police officer and other officers to enter, search, etc.–(*1*) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), any police officer, not below the rank of a [1][Inspector], or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

84A. Modes or methods for encryption.–The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes or methods for encryption.

84B. Punishment for abetment of offences.–Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.
Explanation.–An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.

84C. Punishment for attempt to commit offences.–Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.]

85. Offences by companies.–(*1*) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

(*2*) Notwithstanding anything contained in sub-section (*1*), where a contravention of any of the provisions of this Act or of any rule, direction or order made thereunder has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Power of Police to Investigate

- Section 156 Cr.P.C. : Power to investigate cognizable offences.
- Section 155 Cr.P.C. : Power to investigate non cognizable offences.
- Section 91 Cr.P.C. : Summon to produce documents.
- Section 160 Cr.P.C. : Summon to require attendance of witnesses.
- Section 166A & 166B : Request foreign country

Computer Related Crimes under IPC & Special Laws

Sending threatening messages by email	Sec 503,504 IPC
Sending defamatory messages by email	Sec 499, 500 IPC
Forgery of electronic records	Sec 463, 465, 468, 469 470, 471 IPC
Bogus websites, cyber frauds	Sec 419, 420 IPC
Email spoofing	Sec 416, 417, 463, 465, 468 IPC
Online sale of Drugs	NDPS Act
Web -Jacking	Sec. 383 IPC
Online sale of Arms	Arms Act

Computer Related Crimes under IPC & Special Laws

Theft of electronic device	Sec 379 IPC
Stolen Data/ Data Theft	Sec 411, Sec 379 t 381 IPC
Defamation/Morphing	Sec 469, 499, 500 IPC
Public Mischief	Sec 505 IPC
Publishing indecent materials	Sec 292A, 295A IPC
Deceiving	415 IPC
Falsified Documents	464, 465 IPC
Insult modesty of women	509 IPC

Computer Related Crimes under IPC & Special Laws

Abetment of Suicide (Online)	Sec 305/306 IPC
Cyber Stalking /Bullying of women/children	Sec 354D IPC
Fake Profile	Sec IPC/SLL
Cyber Blackmailing	Sec 384, 503, 506 IPC
Fake News	Sec 505 IPC
Online Gambling	Gambling Act
Online Lotteries	Lotteries Act
Copyright/Trademark copy case	Trademark Act 1999 Copyright Act 1957


LOGOUT

Any Questions

Contact Me

Viralparmarhacker@gmail.com

Facebook.com/viralparmarhacker

Twitter.com/viralparmarhack

Instagram.com/viralparmarhacker

Linkedin.com/in/viral-parmar

www.viralparmarhacker.com

+91 8980808222, +91 8866827872

COMEXPO
CYBER SECURITY
FOUNDATION

Stay Connected

Stay Safe

#LogOutNow