

IT Act 2000 »

Types of Cyber Crimes & Cyber Law in India

(Part-I)

What is a cyber crime?

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web.

There isn't really a fixed definition for cyber crime. The Indian Law has not given any definition to the term 'cyber crime'. In fact, the Indian Penal Code does not use the term 'cyber crime' at any point even after its amendment by the Information Technology (amendment) Act 2008, the Indian Cyber law. But "Cyber Security" is defined under Section (2) (b) means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

What is Cyber Law?

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less of a distinct field of law in the way that property or contract are, as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world, to human activity on the Internet. In India, The IT Act, 2000 as amended by The IT (Amendment) Act, 2008 is known as the Cyber law. It has a separate chapter XI entitled "Offences" in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine.

1. Hacking

What is Hacking?

Hacking is not defined in The amended IT Act, 2000.

According to wiktionary, Hacking means unauthorized attempts to bypass the security mechanisms of an information system or network. Also, in simple words Hacking is the unauthorized access to a computer system, programs, data and network resources. (The term "hacker" originally meant a very gifted

programmer. In recent years though, with easier access to multiple systems, it now has negative implications.)

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(a) read with section 66 is applicable and Section 379 & 406 of Indian Penal Code, 1860 also are applicable. If crime is proved under IT Act, accused shall be punished for imprisonment, which may extend to three years or with fine, which may extend to five lakh rupees or both. Hacking offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

2. Data Theft

What is Data Theft?

According to Wikipedia, Data Theft is a growing problem, primarily perpetrated by office workers with access to technology such as desktop computers and hand-held devices, capable of storing digital information such as flash drives, iPods and even digital cameras. The damage caused by data theft can be considerable with today's ability to transmit very large files via e-mail, web pages, USB devices, DVD storage and other hand-held devices. According to Information Technology (Amendment) Act, 2008, crime of data theft under Section 43 (b) is stated as - If any person without permission of the owner or any other person, who is in charge of a computer, computer system or computer network - 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, then it is data theft.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(b) read with Section 66 is applicable and under Section 379, 405 & 420 of Indian Penal Code, 1860 also applicable. Data Theft offence is cognizable, bailable, compoundable with permission of the court before which

the prosecution of such offence is pending and triable by any magistrate.

3. Spreading Virus or Worms

What is spreading of Virus or Worms?

In most cases, viruses can do any amount of damage, the creator intends them to do. They can send your data to a third party and then delete your data from your computer. They can also ruin/mess up your system and render it unusable without a re-installation of the operating system. Most have not done this much damage in the past, but could easily do this in the future. Usually the virus will install files on your system and then will change your system so that virus program is run every time you start your system. It will then attempt to replicate itself by sending itself to other potential victims.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 43(c) & 43(e) read with Section 66 is applicable and under Section 268 of Indian Penal Code, 1860 also applicable. Spreading of Virus offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

4. Identity Theft

What is Identity Theft?

According to wikipedia Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Information Technology (Amendment) Act, 2008, crime of identity theft under Section 66-C, whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person known as identity theft.

Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else. The term is relatively new

and is actually a misnomer, since it is not inherently possible to steal an identity, only to use it. The person whose identity is used can suffer various consequences when they are held responsible for the perpetrator's actions. At one time the only way for someone to steal somebody else's identity was by killing that person and taking his place. It was typically a violent crime. However, since then, the crime has evolved and today's white collared criminals are a lot less brutal. But the ramifications of an identity theft are still scary.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 66-C and Section 419 of Indian Penal Code, 1860 also applicable. Identity Theft offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

5. E-Mail Spoofing

What is Email Spoofing?

According to wikipedia, e-mail spoofing is e-mail activity in which the sender addresses and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is sending an e-mail to another person in such a way that it appears that the e-mail was sent by someone else. A spoof email is one that appears to originate from one source but actually has been sent from another source. Spoofing is the act of electronically disguising one computer as another for gaining as the password system. It is becoming so common that you can no longer take for granted that the e-mail you are receiving is truly from the person identified as the sender.

Email spoofing is a technique used by hackers to fraudulently send email messages in which the sender address and

other parts of the email header are altered to appear as though the email originated from a source other than its actual source. Hackers use this method to disguise the actual email address from which phishing and spam messages are sent and often use email spoofing in conjunction with Web page spoofing to trick users into providing personal and confidential information.

Law & Punishment: Under Information Technology (Amendment) Act, 2008, Section 66-D and Section 417, 419 & 465 of Indian Penal Code, 1860 also applicable. Email spoofing offence is cognizable, bailable, compoundable with permission of the court before which the prosecution of such offence is pending and triable by any magistrate.

Bibliography:

Author's upcoming book on Cyber Law and Cyber Crimes

...To be continued in Part II, which will be published in the next CSIC issue.