Cyber Crime in India

Cyber Crimes also called computer crime, is any illegal activity that involves a computer or network-connected device, such as a mobile phone. The Department of Justice divides cybercrime into three categories: crimes in which the computing device is the target, for example, to gain network access; crimes in which the computer is used as a weapon, for example, to launch a denial of service (DoS) attack; and crimes in which the computer is used as an accessory to a crime, for example, using a computer to store illegally-obtained data. [Mr Michael Cobb].

The number of cyber crime in India may almost double in 2015 the level of last year. At present, the number of cyber crime in India is nearly around 149,254 and is likely to cross the 300,000 by 2015 growing at compounded annual growth rate (CAGR) of about 107 percent. During 2011, 2012, 2013 and 2014, the total number of cyber crimes registered were 13,301, 22,060, 71,780 and 62,189 (till May) respectively, it said. Source: IBN LIVE

Cyber Crime can be categorized into:

1. The crimes wherein computer is targeted. Examples of such crimes are hacking, virus attacks, stealing of confidential information, etc.

2. The crimes wherein computer is used as a tool. Examples of such crimes are publishing of obscene material, phishing, impersonation, financial frauds, etc.

In India, law as to cyber crimes is contained under Information Technology Act, 2000]. And offences are specifically contained under Chapter 11 of the Information Technology Act - Offences.

Generally, Cyber Crime in India can be:

Cyber Bullying: It involves use of social networks to repeatedly harm or harass other people in a deliberate manner. It mainly includes online harassment of school children.
Cheating by Personation: Impersonation involves trying to assume the identity of another, in order to commit fraud/cheating, including false whois of a website.
Identity Theft: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person.
Obscene Material: Publishing material in the electronic form, which is lascivious or appeals to the prurient interest including pictures of private area of any person or sexual acts online.
Offensive/Harassing Messages: Sending of offensive messages through communication devices and/or social media. In such crimes, mostly women are the target.
Defamation: Online publishing of false statement that harms/damages the good reputation of an individual, group of individuals, brand or a product. Consumer Complaint websites are a good example here.
Cyber Extortion: Extortion is blackmailing another for obtaining, money, property, or services online. For example, defaming a company on a website and demanding money for removal of a complaint.
Hacking: Hacking is unauthorized attempts to bypass the security mechanisms of an information system or network. It is provided under Section 66 of Information Technology Act.
Virus Attacks: Viruses are spread by Cyber Criminals with an objective to hack into a computer system and/or to steal confidential/sensitive information.
Publishing/Circulation of Rumours, especially hurting religious sentiments: Social Media and Mobile messages are used as a tool to spread hatred messages, which may result in violence in a state or a particular part of the country.
Phishing: The act of sending email that falsely claims to be from a legitimate organization, specially Banks. This is usually combined with a request for information: for example, that an account will close, a balance is due, or information is missing from an account. The email will ask the recipient to supply confidential information, such as bank account details, PINs or passwords; these details are then used by the owners of the fake website to conduct fraud.

IPR violations: This involves Software Piracy or otherwise Trademark and Copyright violations like copying of an existing website and/or its content/text is quite common, for which an injunction is required to be taken from court. Also misrepresenting one business with third party's Trademark may be regarding as cheating.
Skimming: It involves fitting an ATM machine with a skimmer device which may reads and records the credit card details on to the device. It results in misuse of credit card and fraud.
Financial Frauds: This may be as a direct result of the above crimes like Hacking, Virus Attack, Extortion, Identity Theft, Skimming, etc.
Cyberstalking: Cyberstalking is the use of the Internet or other electronic means to stalk or harass an individual, a group, or an organization. It may include false accusations, defamation, monitoring, identity theft, threats, or gathering information that may be used to threaten or harass.
Cyber Terrorism: A cyber crime committed with an intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people.

To register a Cyber Crime related complaint, the same should be lodged with a local police station or if available, Cyber Crime Cell in your city. Click here for the Cyber Crime Police Cell location.

News:

#1 Cyber crime FIRs at all police stations (Orissa)

#2 Arrest of Intermediary from Punjab in Domains scam (Pune, Maharashtra)

Articles:

#1 4 types of cybercrime that everyone should know about (]YourStory.com - 2 December 2016)