Monika Bhardwaj,
Anand Wadadekar

CYBER CRIME

Russia, China and Brazil are world leaders in cyber crime. India is fast emerging as a major hub of cyber crime, however our legal system is already in place to tackle this menace of cyber crime and to control it and punish the guilty. Cyber Crime, which we may define as "an unlawful act wherein the computer is either a tool or a target or incidental to the crime

Everyone who works on a computer must be familiar with the term "Cyber Crime". Initially, when man invented computer and then the technology for communicating between computers was evolved, he would have never thought that the cyber space he is creating could be flooded with any crime i.e. cyber crime. But now almost all of us might have heard the term computer crime, cyber crime, e-crime, hi-tech crime or electronic crime which is nothing but an activity done with a criminal intent in cyber space. Simply put, it is an activity which is generally criminal in nature, where a computer or network is the source, tool, target, or place of a crime. To say in one line, "Cyber crime refers to all the activities done with criminal intent in cyberspace."

Such crime involves an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.

This article intends to give an overview of Cyber Crimes since in e-life (of which we all are a part of) conventional crimes like extortion, forgery etc. are being done with the help of computers; which most of us are using for online monetary transactions.

In today's e-Age, 'Crime' has extended itself beyond physical assault or mental torture; now it also affects our e-life. E-Life means our existence & living in the cyber world. Every one of us is a part of this cyber world, directly or indirectly, since computers & internet are now an integral part of our personal & professional life. Just like any other invention, Computers & Internet are a boon to human kind if used in a right way and to the advantage of the society. However, as we all know, everything has its pros and cons and so computers & internet are not an exception. If we consider 'Cyber Crime' as virus then it won't be untrue to say this virus is corrupting man's significant development (computers and internet) which is responsible for developing civilized society for men. Cyber Crime is a menace all over the world and is the one of the most difficult & challenging to detect & investigate. You will find it interesting to note that even the official website of the Cyber Crime Investigation Cell of Crime Branch Mumbai quotes "The invisible criminal is dangerous than the visible one".

Authors
Monika Bhardwaj is B.Com (H), ACS, LL.B
Anand Wadadekar is M.A Eco, MBA Finance, AMFI

You may be wondering why one should know about Cyber Crime?

Most of us are using internet and computers for online transactions where we transmit personal information and possibly do monetary transactions. If your personal information goes in wrong hands and you become bankrupt or you start receiving absurd mails or your e-mail account gets flooded with unwanted mails; means you have become a victim of Cyber Crime.

Cyber Crime has various forms which may include hacking (illegal intrusion into a computer system without the permission of owner), phishing (pulling out the confidential information from the bank / financial institutional account holders by deceptive means), spoofing (getting one computer on a network to pretend to have the identity of another computer in order to gain access to the network), cyber stalking (following the victim by sending e-mails or entering the chat rooms frequently), cyber defamation (sending e-mails to all concerned / posting on website the text containing defamatory matters about the victim), threatening (sending threatening e-mails to victim), salami attacks (making insignificant changes which go unnoticed by the victim), net extortion, pornography (transmitting lascivious material), software piracy (illegal copying of the genuine software / programs), email bombing, virus dissemination (sending malicious software which attaches itself to other software), IPR theft, identity theft, data theft, etc.

Hacking, destroying files and data through spreading virus are the largest number of offences in the cyber world.

"Russia, China and Brazil are world leaders in cyber crime. India is fast emerging as a major hub of cyber crime, however our legal system is already in place to tackle this menace of cyber crime and to control it and punish the guilty. Cyber Crime, which we may define as “an unlawful act wherein the computer is either a tool or a target or incidental to the crime”, has both civil as well as criminal remedies.

So let's talk about the remedies available against such crimes. In India, the offence of Cyber Crime is covered under Information Technology Act 2000 and under the Indian Penal Code.

Cyber Crime Cells have been established by law in major cities. These Cells function directly under the Commissioner of Police of respective cities. Central Bureau of Investigation (CBI) already has a cyber crime wing operational since 1999.

The Government has established “The Cyber Regulations Appellate Tribunal” under the Information Technology Act, 2000. The Tribunal has the same powers as are vested in a Civil Court for requiring the discovery and production of documents, receiving evidence on affidavits. But the decisions of the Tribunal can be contested by the High Court. The Information Technology Act not only applies to the offence committed in India, but it can also be used to bring offenders from foreign countries to India for trial.

Powers of Cyber Crime Cells:

Any police officer, not below the rank of a Deputy Superintendent of Police, 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 or having committed or of committing or of being about to commit any offence under this Act.

Punishment for Cyber Crime:

A person found guilty of cyber crime shall be punishable with imprisonment for a term which may extend to three years or with fine or with both.

Salient features of the Information Technology (Amendment) Act, 2008:

The Information Technology (Amendment) Act, 2008 was enacted in October 2009.

The term “digital signature” has been replaced with “electronic signature” to make the Act more technology neutral. A new section has been inserted to define “communication device” to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image. A new section has been added to define “cyber café” as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.

There is an addition of several new offences into the Act. Section 66 has now been expanded to include sections 66A, (offensive messages) 66B, (Receiving stolen computer) 66C, (Identity theft), 66D (Impersonation), 66E (Voyeurism) and 66 F (Cyber Terrorism). Section 67 has been expanded to include Sections 67A (Sexually explicit content), 67 B (Child Pornography),