Section 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 two three years or with fine which may extend to five lakh rupees or with both.

This means that section 66 is penal provision and 'acts' or 'offences' are listed under section 43 of IT Act, under which the following different 'acts' are listed from 'a' to 'j' sub-sections. It shall be noted that the term 'computer related offences' given under section 66 IT act is vary vast. In order to classify an offence under this section, it is necessary to establish the culprit with dishonest and fraudulent intent had caused destruction, disruption, damage, deletion, denial, concealment, tampering, manipulation,, stealing, alteration, diminishing the value of the information that is in the computer or computer resources.

Section 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;

(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 there under,

(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,

(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) Steals, conceals, 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,

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Under provision 43, sub-section 'a' cases of hacking (unauthorised access), website defacement are covered. Under sub-section 'b' downloading, copying protected information are covered. Infecting a computer with virus or computer contaminant is punishable under sub-

section ‘c’. Similarly different general offences that are related to computers are covered.

"Computer Contaminant" means any set of computer instructions that are designed - (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network;

"Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

It is important to note that the term ‘hacking’ per se is not defined under Information Technology Act, nevertheless, the section 66 read with 43 sub-section (a) is the relevant provision for authorised access which is otherwise hacking.

A case of hacking – standard operating procedure (SOP):-

The following standard operating procedures (SOPs) may be followed in a case of hacking which is un-authorised access of a computer resource.

- As per the ingredients mentioned under section 43 sub-class ‘a’, if any person without the permission of the owner or without the permission of the person who is in-charge of the such computer, accesses such computer then it is an offence punishable under section 66 I T At. Therefore this section is applicable for unauthorised access which is otherwise known as ‘hacking’.

- To establish un-authorised access the computer system logs may be collected. Computer system logs may include web logs, server logs, file transfer protocol (FTP) log, firewall logs. These logs may be

analysed and the IP Addresses that are associated with the un-authorised access may be identified and collected on a compact disk under the cover of mediator report. This analysis can be done with the help an expert and such proceedings may be recorded.

- The concerned people who manage the server / computer that was hacked need to be examined and their statements are to be recorded incorporating the facts: what were the security measures on place, when the hacking was realised? Etc

- After identification of the suspected IP Addresses, the source of such IP Addresses can be traced with the information provided by the Internet service providers.

  The IP Addresses may be searched for lookup on websites like www.apnic.net, www.domaintools.com, www.whois.net etc the IP Address assignee, which can be usually am Internet Service Provider (ISP) information may be ascertained.

  In the next step by writing or by sending an email request to the ISP the end user details of the IP Addresses may be collected and thereby the name and address of the person who has made unauthorised access is known.

- Thus the suspect can be identified and he may be questioned and if he admits, his confession may be recorded before mediators and in pursuance of such confession and, at the instance of the culprit the tool of offence which could be a computer, laptop or mobile phone that was used for committing the offence may be recovered.

- The recovered tool of offence (computer, laptop or mobile) may be forwarded to the Forensic Science Laboratory (FSL) under a Letter

of Advice with a proper relevant questionnaire and a analysis report may be obtained.

The specific question, to the expert in these cases is to analyse the MO for the presence of an IP, any tool of hacking or any linking electronic evidence between the hacker computer and the target computer and to retrieve the same and furnish.

- In these cases the IO can also recover the gadget i.e., data card etc that is used by the accused, to access Internet. Examination of the nodal officer of the ISP is also required.

- Thus the case may be established with proper documentary (electronic), oral, circumstantial, scientific evidences.

  - Cases of website defacement will also come under this category, hence a similar line of investigation may be followed to trace the culprits.

If the IP Address leads to a foreign country the procedure of issuing Letter of Request (Letter Rogatory) as per section 166-A Criminal Procedure Code and the guidelines issued by Central Bureau of Investigation (CBI) at http://cbi.nic.in/interpol/invletterrogatory.php shall be followed to secure information / evidences from other countries.

***