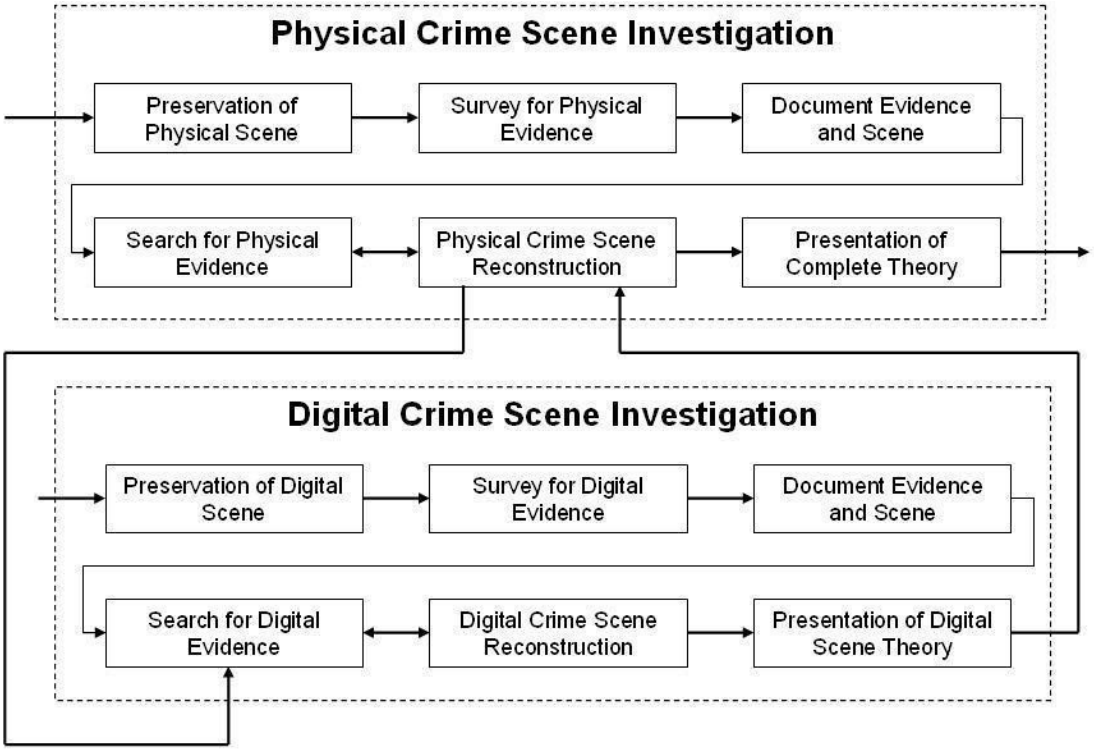
Lecture- 34

Online hate community	It is created for provoking a religious group to act or pass obnoxious/ objectionable remarks against a public figure or the country etc. Applicable provisions: Section 66A of IT Act + 153A & 153B of the Indian Penal Code (IPC)
Email account hacking	If a person's email account is hacked and offensive / indecent emails are sent to people who are in person's address book. Applicable provisions: Sections 43, 66, 66A, 66C, 67, 67A and 67B of IT Act.
Web defacement	The Website's homepage is swapped with a defamatory or pornographic content/ page. Applicable provisions: Sections 43 and 66 of IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.
Cyber terrorism	The terrorists are using virtual & physical storage for hiding data & records of their illegal business. Applicable provisions: terrorism laws apply + Section 66F & 69 of IT Act.
Phishing and email scams	It involves acquiring sensitive information fraudulently by masquerading as a reliable & legitimate entity. Applicable provisions: Section 66, 66A and 66D of IT Act + Section 420 of IPC

One can report a cyber-crime by:

- Filing a written complaint in nearest, any Cyber Cell
- Lodging an F.I.R (First Information Report)
- Filing a complaint at https://www.cybercrime.gov.in/Accept.aspx

After filing of a complaint / F.I.R., the process of investigation, is hereby diagrammatically presented below:



Source: ht tp://www.dynotech.com/articles/images/crimescene.jpg

In case the response has not been appropriate then the complainant can write to State / UT Nodal Officer and Grievance Officer, the details of which can be accessed here: https://www.cybercrime.gov.in/Webform/Crime_NodalGrivanceList.aspx.

Recently, for Delhi only, a new feature "**Citizen Financial Cyber Fraud Reporting and Management System**" has been activated for prevention of money loss in case of Cyber Financial Fraud; for immediate reporting the complainant can Call 155260 (9 AM – 6 PM only) and further details can be accessed from 'Citizen Manual' under "Resources Section" at www.cybercrime.gov.in.

Prosecution for cyber-crimes

Some common cyber-crimes incidents which attracts prosecution as per the applicable provisions of the IT Act, are provided herein below:

Conclusion

The Indian Computer Emergency Response Team (CERT-In) is the national nodal agency established by the Ministry of Electronics & Information Technology (MeitY), Government of India, for responding to computer security incidents & securing the Indian cyber space. In the year 2019, CERT-In handled 3,94,499 incidents. The incidents handled were:

- Website Intrusion & Malware Propagation
- Malicious Code
- Phishing
- Distributed Denial of Service attacks
- Website Defacements

- Unauthorized Scanning activities and vulnerable service.

The CERT-In has executed a Memorandum of Understanding on cyber security co-operation with Finland, Estonia & South Korea, to strengthen & enable information sharing & collaboration for incidents resolution.

The MeitY has also launched “Cyber Swachhta Kendra” (Botnet Cleaning and Malware Analysis Centre), to detect the botnet infections and create a secure cyberspace in India. This centre is being operated by the CERT-In as per the provisions of Section 70B of the IT Act.