Cyber Crime on Vulnerable Internet

Komakula Sivaji, Inspector of Police, CCPS., VJA.
Topics

What is Internet?
What is Cyber Crime?
How a crime takes place in Cyber Space?
Types of Cyber Crimes?
Investigation
INTERNET

a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.
CYBER CRIME

Any offence committed by using any electronic device as a tool or as a target.
Ex: Mobile, Tab, Laptop, Desk Top etc.
Offence with Internet

- Every cyber crime will be connected to the internet
- Even to send a SMS through basic mobile, it needs some network which connects to internet and deliver the same one place to another place.
- It requires two objects – one is to send and another one is to receive
Types of Cyber Crimes

S – H – O

- Source Code Theft
- Hacking
- Obscenity
Types of Cyber Crimes

- Financial Frauds like...
  - O.T.P. fraud
  - Shoulder surfing
  - ATM Frauds
  - Fake Job frauds
  - Lottery/Gifts/Loan
  - Online Sales and purchases OLX.
  - Matrimonial Frauds

- Cyber Stalking - Harassment or Blackmail through Social media

- Cyber Terrorism
Source Code

- It is Unique for each and every programme
- Stealing the Source code is an offence
- Ex-employees
- Competitors
HACKING

- Stealing the Identity
- Accessing others privacy
- Gaining access into un-authorised area in digital world
- Misusing the information
- Computing – modifying – tampering – Forgery
- Dishonest intention – wrongful loss – wrongfull gain
transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form

publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.
INVESTIGATION

- Examination of PWs.
- Collection of basic evidence
- Analysation
- Identifying the sources of evidence
TYPES OF LEADS

- M.S.P.s/C.D.Rs
  - frequent callers
  - Frequent towers
  - Service messages
  - IMEIs
- I.S.P.s/I.P. Addresses
- Banks
- Intermediary agencies
- Gateways
- E-merchants
TYPES OF LEADS contd…

- Godaddy
- U.R.Ls
- Intermediary agencies to stop the publication /transmission u/s 79 IT Act.
PHYSICAL EFFORTS

- Analysing the DATA collected
- Identifying and pinpointing the accused.
- Tracking the accused.
- Time to time info.
- Cooperation of local police
- Preparation of record
- Execution of arrest
Information Technology (Amendment) Act 2008

- Definitions
- Penal Sections
- Amendments to IPC & IEA
- Case Studies
Sec. 65 : Tampering with the Computer Source Documents

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh, rupees, or with both.
Computer Source Code: Means the listing of programmes, computer commands design and layout.
Sec 66: 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 three years or with fine which may extend to rupees five lakh rupees or with both.
Sec 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 database 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 database 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

(i) 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.
Punishment for sending offensive messages through communication service, etc.

66 A: Any person who sends, by means of a computer resource or a communication device,—

(a) Any information that is grossly offensive or has menacing character; or

(b) Any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.
Punishment for dishonestly receiving stolen computer resource or communication device

66 B: Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
Punishment for identity theft

66C: Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.
66D: Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee.
66E: Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
Punishment for cyber terrorism.

66F: 1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or
(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorized access; or
(iii) introducing or causing to introduce any Computer Contaminant.

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or
(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life‘.
Sec. 67: Publishing of information, which is obscene in electronic form

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it,

shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.
67A: Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form

67B. Whoever,—

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.
Sec. 77 B: Offences with three years imprisonment to be bailable.

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.
Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of a Inspector shall investigate any offence under this act.
“This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource.”
“This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed.”
“Virus is a program that attaches itself to a computer or a file and then circulates to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.”
“Web jacking is the act of cracking and changing a website’s admin passwords and then taking control of the website. The motive is usually money.”
Victims are sent unsolicited e-mails mentioning luring content that they have own lottery or unclaimed money in bank to be claimed etc, if the victims are fall prey to such temptations amounts are squeezed from them on various false pretexts i.e., payment of Advance Fee, courier chargers etc.
Using spoof e-mails and directing people to fake websites to fool them into divulging personal / financial details so criminals can access their accounts.

Nearly 8 million phishing attacks per day.
Credit and Debit card fraud is a theft and fraud committed by misusing a credit or debit card as a fraudulent source of payment in a transaction.

The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.
Thank “U”

Komakula Sivaji,
Inspector of Police,
Cyber Crimes P.S.