Cyber Security

Subject Code:-102045607

Unit-6 Introduction about Cyber Crime and Cyber Security

Introduction about Cyber Crime and Cyber Security

Cyber crimes are majorly of 4 types:

1. Against Individuals: These include e-mail spoofing, spamming, cyber defamation, cyber harassments and cyber stalking.
2. Against Property: These include credit card frauds, internet time theft and intellectual property crimes.
3. Against Organisations: These include unauthorized accessing of computer, denial Of service, computer contamination / virus attack, e-mail bombing, salami attack, logic bomb, trojan horse and data diddling.
4. Against Society: These include Forgery, CYber Terrorism, Web Jacking.

Introduction about Cyber Crime and Cyber Security

(1) Cyber crime against Individual

(i) Email spoofing : A spoofed email is one in which the e-mail header is forged so that the mail appears to originate from one source but actually has been sent from another source.

(ii) Spamming : Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.

(iii) Cyber Defamation : This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information.

(iv) Harassment & Cyber stalking : Cyber Stalking Means following an individual's activity over internet. It can be done with the help of many protocols available such as e- mail, chat rooms, user net groups.

Introduction about Cyber Crime and Cyber Security

(2) Against Property

I. **Credit Card Fraud :** As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.

II. **Intellectual Property crimes :** These include Software piracy: Illegal copying of programs, distribution of copies of software. Copyright infringement: Using copyrighted material without proper permission. Trademarks violations: Using trademarks and associated rights without permission of the actual holder. Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

III. **Internet time theft :** This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

Introduction about Cyber Crime and Cyber Security

(3) Against Organisations

(i) Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner. It can be of 2 forms: a) Changing/deleting data: Unauthorized changing of data. b) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

(ii) Denial Of Service : When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

(iii) Computer contamination / Virus attack : A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to

Introduction about Cyber Crime and Cyber Security

(3) Against Organisations

(iv) Email Bombing : Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.

(v) Salami Attack : When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes.

(vi) Logic Bomb : It is an event dependent program. As soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

Introduction about Cyber Crime and Cyber Security

(4) Against Society

(i) Forgery : Currency notes, revenue stamps, mark sheets etc. can be forged using computers and high quality scanners and printers.

(ii) Cyber Terrorism : Use of computer resources to intimidate or coerce people and carry out the activities of terrorism.

(iii) **Web Jacking** :Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

The legal perspectives

Section 67 of the Information Technology Act, 2000 in parallel to Section 292 of Indian Penal Code, 1860 makes publication and transmission of any material in electronic thats lascivious or appeals to the prurient interest a crime, and punishable with imprisonment which may extend to 5 years and fine of 1 lakh rupees and subsequent offence with an imprisonment extending to 10 years and fine of 2 lakhs.

Indian ITA 2000

- The Information Technology Act, 2000 also Known as an **IT Act** is an act proposed by the Indian Parliament reported on 17th October 2000.
- This Information Technology Act is based on the United Nations Model law on Electronic Commerce 1996 (UNCITRAL Model) which was suggested by the General Assembly of United Nations by a resolution dated on 30th January, 1997.
- It is the most important law in India dealing with Cybercrime and E-Commerce.

Indian ITA 2000

- The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes.
- The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

Indian ITA 2000

The offences and the punishments in IT Act 2000 :

The offences and the punishments that falls under the IT Act, 2000 are as follows :-

- Tampering with the computer source documents.
- Directions of Controller to a subscriber to extend facilities to decrypt information.
- Publishing of information which is offensive in electronic form.
- Penalty for breach of confidentiality and privacy.
- Hacking for malicious purposes.
- Penalty for publishing Digital Signature Certificate false in certain particulars.
- Penalty for misrepresentation.

Indian ITA 2000

The offences and the punishments in IT Act 2000 :

The offences and the punishments that falls under the IT Act, 2000 are as follows :-

- Power to investigate offences.
- Protected System.
- Act to apply for offence or contravention committed outside India.
- Publication for fraud purposes.
- Power of Controller to give directions.

Indian ITA 2000

Sections and Punishments under Information Technology Act, 2000 are as follows :

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	This section of IT Act, 2000 states that any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.
Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.

Indian ITA 2000

Sections and Punishments under Information Technology Act, 2000 are as follows :

SECTION	PUNISHMENT
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine of Rs. 10,00,000 or both.

Cyber-crime: A Global Perspective

- Cybersecurity constitutes one of the top five risks of most firms, especially in Big Tech and Banking & Financial Services.
- Global cybercrime damage costs this year are expected to breach US $6 trillion an annum. That is almost one-fourth of the US GDP or twice the GDP of India.
- This is expected to scale up to US $10.5 trillion an annum by 2025. Cyber attackers are disrupting critical supply chains, at least 4 times more than in 2019.

Thank you!