Cyber Crime, Cyber Security and Cyber Rights in INDIA

Ms. Jyoti Lakhani

Head, Department of Computer Science

Maharaja Ganga Singh University, Bikaner

Cyber Crime

ANY "CRIMINAL ACTIVITY" PERFORMED USING COMPUTER

Electronic Crime

e-Crime

It's an "*UN-LAWFUL ACT*" wherein the computer is either a tool or a target or both

First Occurrence of Cyber Crime

- The first spam email took place in 1978 when it was sent out over the Arpanet (Advanced Research Projects Agency Network)

- The first virus was installed on an Apple computer in 1982 when a high school student, Rich Skrenta, developed the Elk cloner

Categories of Cyber Crime

Cyber crimes against Persons

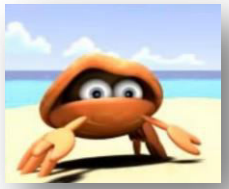
Cyber crimes against Property

Cyber crimes against Government

Cyber crimes against Society

Cyber-Criminals

Cyber-Criminals



Insider threat

Employees itself

An **Insider threat** is a malicious threat to an organization

Comes from people within the organization, such as employees, former employees, contractors or business associates

Who have inside information concerning the organization's security practices, data and computer systems

Cyber-Criminals

Hackers

A **hacker** is someone who seeks and exploits weaknesses in a computer system or computer network

Cyber-Criminals

Hactivist

(overloads e-mail servers or hack web sites to send political message)

Cyber-Criminals

Virus writers

(writes viruses to infect systems)

Cyber-Criminals

Criminal groups

(attack systems & steal password for financial gain)

Cyber-Criminals

Sensitive intrusions

(sensitive information is obtained via computer intrusions)

Cyber-Criminals

Information warfare

(alternative to military attacks)

Cyber-Criminals

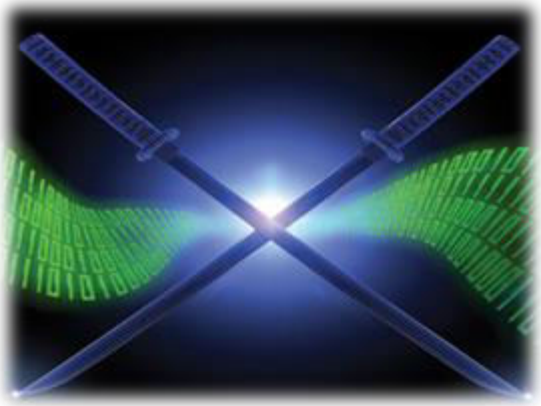
Terrorists

(who have potential to disrupt government systems with computer attacks)

Cyber-Criminals

Cyber Warfare

(attack by sovereigns ---
Crime or Declaration of war)



ATTACK

Weapons Cyber Crime

Hacking

Unauthorized access to any computer systems or networks is known as ‘HACKING’. That is accessing the information of others without proper authorization.

Weapons of Cyber Crime

Data Diddling

This is altering raw data just before a computer processes it and then changing it back after the processing is completed.

Weapons of Cyber Crime

Denial of Service Attack

The computer is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDOS) attack is a example.

Weapons of Cyber Crime

Email Bombing

It refers to sending large numbers of mail to the victim, which may be an individual or a company by ultimately resulting into crashing.

Weapons of Cyber Crime

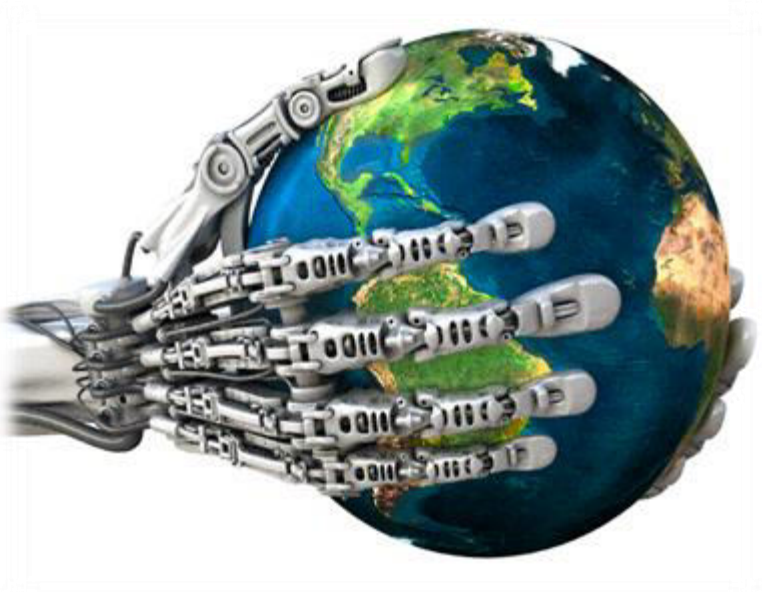
Trojan Attacks

This term has its origin in the word ‘Trojan horse’. In software field this means an unauthorized program, which passively gains control over another’s computer by representing itself as an authorized program. The most common form of installing a Trojan is through e-mail.

Weapons of Cyber Crime

Web Jacking

This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the website of another. He may even manipulate or change the information of the website. This may be done for fulfilling political objectives or for money.



Weapons of Cyber Crime

Virus Attack

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it

Weapons of Cyber Crime

Worm Attacks

Worms unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on the computer's memory.

Weapons of Cyber Crime

Salami Attacks

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.

Weapons of Cyber Crime

Phishing

Phishing refers to the receipt of unsolicited emails by customers of Financial Institutions, requesting them to enter their Username, Password or other personal information to access their Account for some reason. The fraudster then has access to the customer's online bank account and to the funds contained in that account.

Weapons of Cyber Crime

Spamming

Electronic spamming is the use of electronic messaging systems to send unsolicited bulk messages (**spam**), especially advertising, indiscriminately. The most widely recognized form of spam is e-mail spam.

Weapons of Cyber Crime

Cyber stalking is the use of the internet or other electronic means to stalk someone. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly.

Cyber Crimes Against Persons

Harassment via E-Mails *(**Email harassment*** is the act of consistently sending unwanted electronic communications to a person to intimidate, frighten, or...*)*

Hacking

E-Mail / SMS Spoofing *(**E-mail spoofing*** is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.*)*

Carding*(False credit card/debit card etc.)*

Assault by Threat *(threatening)*

Cyber Crimes Against Property

Intellectual Property Crimes *(*Criminal offences (counterfeiting and piracy) Infringement of trade marks and copyrights can be criminal offences)

Cyber Squatting *(*is registering, trafficking in, or using a domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else.)

Cyber Vandalism *(**Cyber vandals*** are individuals who damage information infrastructures purely for their own enjoyment and pleasure. Their primary motivation is not financial;*)*

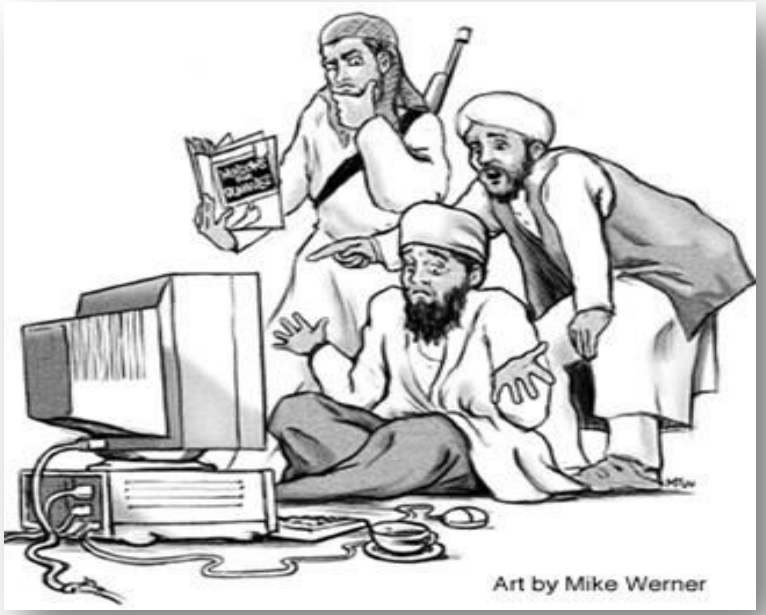
Transmitting Virus

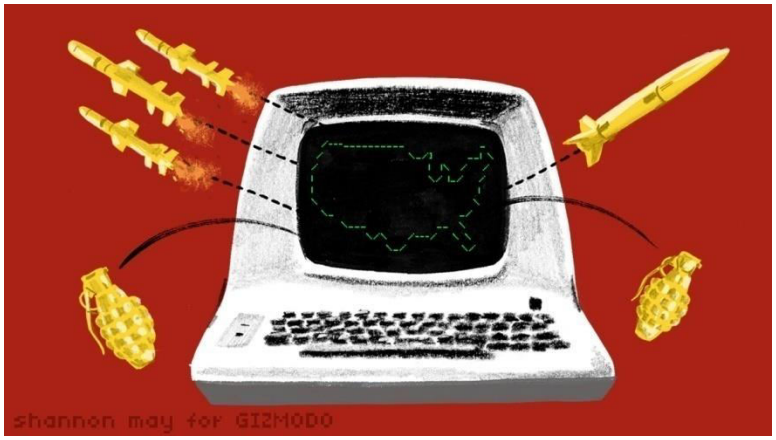
Internet Time Thefts - ***Internet time theft*** comes under the heading of hacking. It is the use by an unauthorized person of the Internet hours paid for by another person.

Cyber Crimes Against Government

Cyber Terrorism:

Cyber Terrorism is a phrase used to describe the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.





Cyber crimes Against Society

Cyber Trafficking Drug ***traffickers*** are increasingly taking advantage of the Internet" according to ***cyber*** authorities and personnel. to sell their illegal substances through encrypted

Online Gambling *(*gambling using the Internet.)

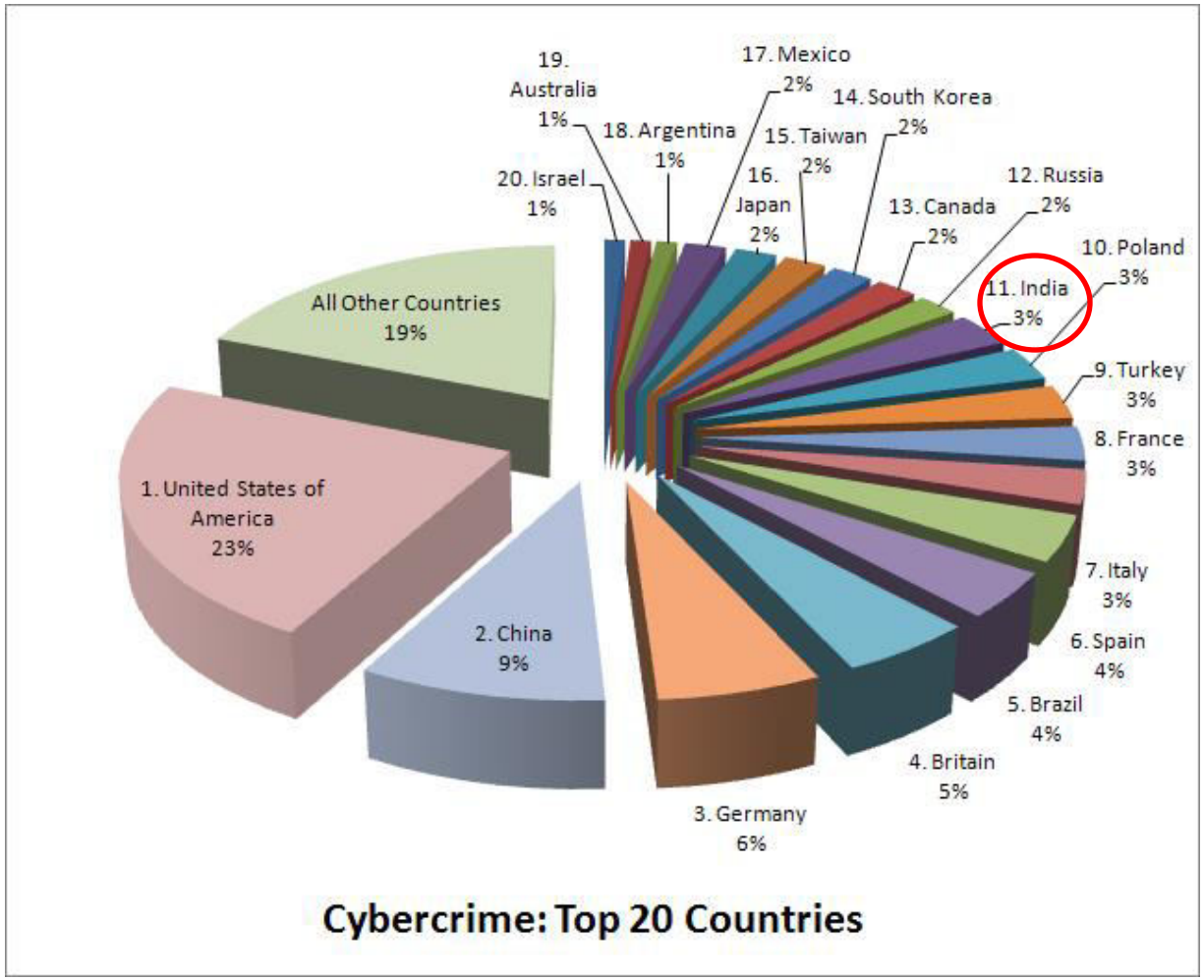
Forgery - person is guilty of ***forgery*** if he or she makes a false instrument with the intention that it shall be used to induce another person t… by reason of so accepting it, to do some act, or to ma… prejudice of that person or any other person.

CYBER CRIME

IN

INDIA

Cyber Crime in INDIA



Cyber Crime in India Some Facts

- India is the third-most targeted country for Phishing attacks after the US and the UK
- The majority of cybercrimes are centered on forgery, fraud and Phishing
- Social networks as well as ecommerce sites are major targets
- 6.9 million bot-infected systems in 2013
- 14,348 websites defacements in 2013
- 15,000 sites hacked in 2013
- India is number 1 country in the world for generating spams.
- 29.9 million people fell victim to cyber crime.
- 17% of adults online have experienced cybercrime on their mobile phone.

•Source: Norton Cybercrime Report 2013

WHY INDIA?

- India : world's third largest Internet user after China and the US
- Younger Users
- 74 million Active Internet users
- 46+ Million Social Network Users
- 50 Million users shop online on Ecommerce and Online Shopping Sites
- 164.81 million Internet subscribers (as on March 31, 2013)
- seven out of eight accessing the Internet from their mobile phones.

Cyber Security and Right to Privacy

"The Information Technology Act 2000 contains adequate provisions to deal with various cyber related offenses as well as protection of privacy of individuals.

IT Act 2000

Crime: **Cyber Stalking**

Definition: Stealthily following a person, tracking his internet chats.

Mechanism: By using electronic communication, such as e-mail instant messaging (IM), messages posted to a Web site or a discussion group.

Sections and Amendments: 43, 66
(Compensation and punishment of three years with fine)

Technical Measures: Not disclosing personal information on Internet, chat, IM and interacting over electronic media with known people only.

•Taking up the matter with concerned Service Providers in stopping cyber stalking activities.

IT Act 2000

Crime: **Intellectual Property Crime**

Definition: Source Code Tampering etc.

Mechanism: Accessing source code or such type of material and stealing or manipulating the code etc.

Sections and Amendments: 43, 65, 66
(Compensation and punishment of three years with fine)

Technical Measures: Strong authentication and technical measures for prevention of data leakage

IT Act 2000

Crime : **Salami Attack**
(Theft of data or manipulating banking account)

Definition:Deducting small amounts from an account without coming in to notice, to make big amount

Mechanism: By means of unauthorized access to source code of software application and databases

Sections and Amendments: 43, 66
(Compensation and punishment of three years)

Technical Measures: Strong authentication measures for accessing the data and securing the IT infrastructure involved

IT Act 2000

Crime: **E-Mail Bombing**

Definition:Flooding an E-mail box with innumerable number of E-mails, to disable to notice important message at times.

Mechanism: Bulk email generation to target specific email account by using automated tools

Sections and Amendments: 43, 66
(Compensation and punishment of three years)

Technical Measures: Implementing anti-spam filters

IT Act 2000

Crime: **Phishing**

Definition: Bank Financial Frauds in Electronic Banking

Mechanism: Using social engineering techniques to commit identity theft

Sections and Amendments: 43, 66, 66C
(Compensation and punishment of three years with fine)

Technical Measures: Immediate take-down of phishing websites.
- Strong authentication mechanisms for financial and electronic banking.
- User awareness on phishing attacks
- Keeping the computer systems secure being used for transacting with the financial institutions and banks.

IT Act 2000

Crime: **Personal Data Theft**

Definition:Stealing personal data

Mechanism:Compromising online personal data, email accounts and computer systems

Sections and Amendments: 43, 43A, 72A
(Compensation and punishment of three years with fine)

Technical Measures: Safeguarding the online data and personal computer systems

IT Act 2000

Crime: **Identity Theft**

Definition:Stealing Cyberspace identity information of individual

Mechanism:Hacking the personal identity information or employing phishing techniques

Sections and Amendments: 43
(Compensation and punishment of three years with fine)

Technical Measures: Safeguarding of personal identity information, securing the personal computer systems, awareness on preventing identity theft and adopting safe internet practices

IT Act 2000

Crime: **Spoofing**

Definition:Stealing Credentials using, friendly and familiar GUI's

Mechanism:Using tools and other manipulative techniques

Sections and Amendments: 43, 66
(Compensation and punishment of three years with fine)

Technical Measures: Safeguarding the credentials and implementing anti-spoofing measures

IT Act 2000

***Crime*: Data Theft**

Definition:Stealing Data

Mechanism:Hacking of computer systems and using malicious methods

Sections and Amendments: Provisions under 43, 43A, 65,66 and 72 (Compensation and punishment of three years with fine)

Technical Measures: Securing the computer systems, implementing data leak prevention measures and creating user awareness

IT Act 2000

Crime: **Worms Trojan Horses, Virus etc.**

Definition:Different Hacking mechanisms

Mechanism:Different methods to install and propagate malicious code

Sections and Amendments: 43, 66
(Compensation and punishment of three years with fine)

Technical Measures: Securing computer systems, installing anti-malware systems and creating user awareness.

IT Act 2000

Crime: **Sabotage of Computer**

Definition:Taking control of computer with the help of malware.

Mechanism:Compromising the computer systems

Sections and Amendments: 43, 66
(Compensation and punishment of three years with fine)

Technical Measures: Securing computer systems and deploying anti-malware solution

IT Act 2000

Crime: **DOS, DDOS Demat of Service**

Definition:Flooding a computer with Denial of Service Attacks, DDOS is Distributed DOS attack

Mechanism:Generating flood traffic from thousands and millions of compromised computers using automated tools and techniques

Sections and Amendments: 43, 66, 66F
(Compensation (up to life imprisonment under 66F)

Technical Measures: Implementing DOS, DDOS prevention systems

IT Act 2000

Crime: **Web Defacing**

Definition:Web Pages Defacing

Mechanism:Compromising the websites and adding or manipulating the web pages with some messages

Sections and Amendments: 43, 66
(Compensation and punishment of three years with fine)

Technical Measures: Securing the websites and the IT infrastructure used for hosting and maintaining the websites

IT Act 2000

Crime: **Spam and spoofing**

Definition:Unsolicited E-mails

Mechanism:Sending unsolicited emails through manual and automated techniques

Sections and Amendments: 43, 66A, 66D
(Compensation and punishment of three years with fine)

Technical Measures: Deploying the anti-spam and anti-spoofing solution at email gateways

IT Act 2000

Crime: **Publishing or transmitting obscene material**

Definition:Publishing Obscene in Electronic Form

Mechanism:Publishing or transmitting the obscene content over electronic media like websites, social networking sites etc.

Sections and Amendments: 67
(Punishment of three years with fine)

Technical Measures: Taking down of obscene materials over electronic media

IT Act 2000

Crime: **Pornography**

Definition:Publishing or transmitting material containing sexually explicit act

Mechanism:Publishing pornographic material over electronic media like websites, social networking sites etc.

Sections and Amendments: 67A
(Punishment of five years with fine)

Technical Measures: Taking down of pornographic material publishing websites/ web-pages, online media etc.

IT Act 2000

Crime: **Child Pornography**

Definition:Publishing Obscene in Electronic Form involving children

Mechanism:Publishing pornographic material involving children over electronic media like websites, etc.

Sections and Amendments: 67B

Technical Measures: Taking down of pornographic material publishing websites/ web-pages, online media etc.

IT Act 2000

Crime: **Video Voyeurism and violation of privacy**

Definition:Transmitting Private/ Personal Video's on internet and mobiles

Mechanism:Transmitting Private/Personal Video's on internet and mobiles

Sections and Amendments: 66E
(Punishment of three years with fine)

Technical Measures: Taking down of such content as available over internet and transmitted through mobiles.

IT Act 2000

Crime: **Offensive messages**

Definition:Transmitting Private/ Personal Video's on internet and mobiles

Mechanism:Transmitting Private/Personal Video's on internet and mobiles

Sections and Amendments: 66E
(Punishment of three years with fine)

Technical Measures: Taking down of such content as available over internet and transmitted through mobiles.

IT Act 2000

Crime: **Offensive messages**

Definition:Communication of offensive messages through computer/ phone

Mechanism:Sending or publishing the offensive messages over electronic media like email, websites and social media

Sections and Amendments: 66A
(Punishment of three years with fine)

Technical Measures: Taking down of offensive messages from electronic media and creating user awareness on safe internet practices

IT Act 2000

Crime: **Hacking of Protected Systems**

Definition:Protection of Information Infrastructure

Mechanism:Hacking the computer systems by using various methods

Sections and Amendments: 70
(Punishment of ten years with fine)

Technical Measures: Securing the computer systems and related infrastructure, creating user awareness and training of system administrators

PREPAREDNESS AND POLICY INITIATIVES

WHAI IF the systems like defence establishments, hospitals, transportation, Banks, Government organisations, etc., are hijacked or manipulated through cyber attacks.

The Government has taken several actions to improve the alertness of the Government and other critical sector organisations.

‘Crisis Management Plan’ (CMP)

For countering cyber attacks and cyber terrorism

-All Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors have been mandated to continuously assess the posture of their IT systems and networks.

-The CMP mandates following specific steps:

1. Nominate Chief Information Security Officers to co-ordinate the security related issues/implementation within the organisation

‘Crisis Management Plan’ (CMP)

2. Security devices may be installed at all levels. Servers, Local Area Network (LAN) and Wide Area Network (WAN) infrastructure should be secured by installing appropriate perimeter security devices such as firewalls, Intrusion Prevention System and anti-virus system.

3. These security mechanisms should include appropriate devices and methods to log and monitor the events to detect network scanning, probing and Reconnaissance attempts on the IT infrastructure.

‘Crisis Management Plan’ (CMP)

4. These attempts should be regularly reviewed and analysed for initiating necessary preventive measures.

5. Deployment of network traffic scanning technique to improve the visibility into the state of the network and identifying deviations from baselines that may indicate abnormal or suspicious behaviour.

Safety Tips to avoid cybercrime

- Keep your operating systems up to date with critical security updates and patches.
- Don’t open emails or attachments from unknown sources.
- Read Privacy policy carefully when you submit the data through internet.
- Disable Remote Connectivity.
- Use hard-to-guess passwords. Don’t use words found in a dictionary. Remember that password cracking tools exist.
- Back-up your computer data on disks or CDs often.
- Use antivirus software and firewalls –keep them up to date