INTRODUCTION TO

CYBER SPACE
CYBER CRIME
CYBER LAWS
CYBER SECURITY

CYBER SPACE

- Environment that involves interactions between people, software, and services.

- MAINTAINED BY WHOM

- INCLUDES : computers, networks, software, data storage devices (e.g., hard disks), the internet, websites, emails and also includes even electronic devices such as Cell Phones, ATM Machines etc.

DEFINING CYBER SPACE

- A Virtual Medium
- 24x7x365

ALSO

Cyberspace is a space based on bits and bytes.

CYBER SECURITY

- Denotes the technologies and procedures to safeguard resources from unlawful admittance through the Internet.

- ISO 27001 (ISO27001) International Cyber Security standard for managing IS management system.

CYBER SECURITY POLICY

- an authority framework that defines and guides the activities associated with the security of cyberspace.

- Provides an outline to effectively protect information, information systems and networks.

- Manages the entire field of ICT users and providers.

CYBER CRIMES

- Crimes directed at a computer or a computer network.

- Regulatory mechanism in cyberspace.

CYBER CRIME

- **Computer crime/ cyber crime/electronic crime/ hi-tech crime** normally refers to a criminal activity where computer or network is used as a tool or target of a crime.

- **Computer as a tool :**When individual is the main target of the crime committed by the offenders then the computer can be described as a tool and not the target (*e.g.*, *cyber stalking, cyber theft etc.).*

- **Computer as a target :**These crimes are committed by a selected group of people with technical knowledge by committing a series of acts in the planned manner (*e.g.*, *web defacement, cyber* terrorism etc.).

CATEGORIES

Categories of Cyber Crimes

| Cyber Crimes against Persons | Cyber Crimes against Property | Cyber Crimes against Government/ Firm/ Company/ Group of Individuals | Cyber Crimes against Society |

CATEGORIES OF CYBER CRIME

- **Cyber crimes against persons(**include harassment of someone with the use of a computer **)**

- **Cyber crimes against property (**intellectual property crimes, cyber vandalism **)**

- **Cyber crimes against government/firm/company/group of individuals(**include cyber terrorism ,pyrated software distribution**)**

- **Cyber crimes against society (**online gambling, selling Illegal articles**)**

KINDS OF CYBER CRIME

UNAUTHORIZED ACCESS AND HACKING

- **Unauthorized access** refers to any kind of access Without seeking the permission of either the true owner or the person in charge of a computer

- **Hacking** / **cracking** is a crime for gaining unauthorized access to the data stored in system.

- Under IT ACT 2000 , the punishment for a hacker is imprisonment for a period of 3 years or fine which may extend to ₹2 lakhs or both.

- **PURPOSE** personal monetary gain (e.g., stealing of credit card information and transferring the proceeds to their account and then withdrawal of that money).

VIRUS, WORMS AND TROJAN ATTACK

VIRUS
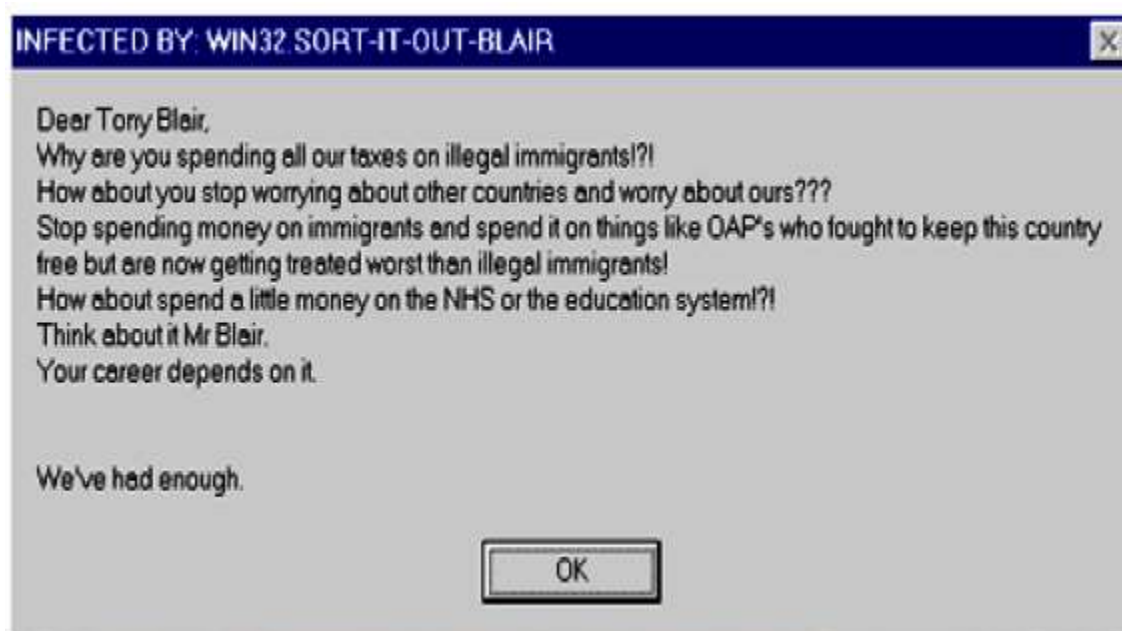
- A program that is capable of infecting other program and making copies of itself.
- **Designed** to replicate as well as spread.

WARNING: Virus Detected!

VIRUS NAME: TAPSNAKE

Security Risk:

Infected File: /os/apps/snake.icv

Description: Steals passwords and credit card information.

VIRUS, WORMS AND TROJAN ATTACK

WORMS

- **Programs that multiply like viruses but spread from one computer system to another.**

- **Not required to attach themselves to a host programme.**

INFECTED BY: WIN32.SORT-IT-OUT-BLAIR

Dear Tony Blair,
Why are you spending all our taxes on illegal immigrants!?!
How about you stop worrying about other countries and worry about ours???
Stop spending money on immigrants and spend it on things like OAP's who fought to keep this country free but are now getting treated worst than illegal immigrants!
How about spend a little money on the NHS or the education system!?!
Think about it Mr Blair.
Your career depends on it.

We've had enough.
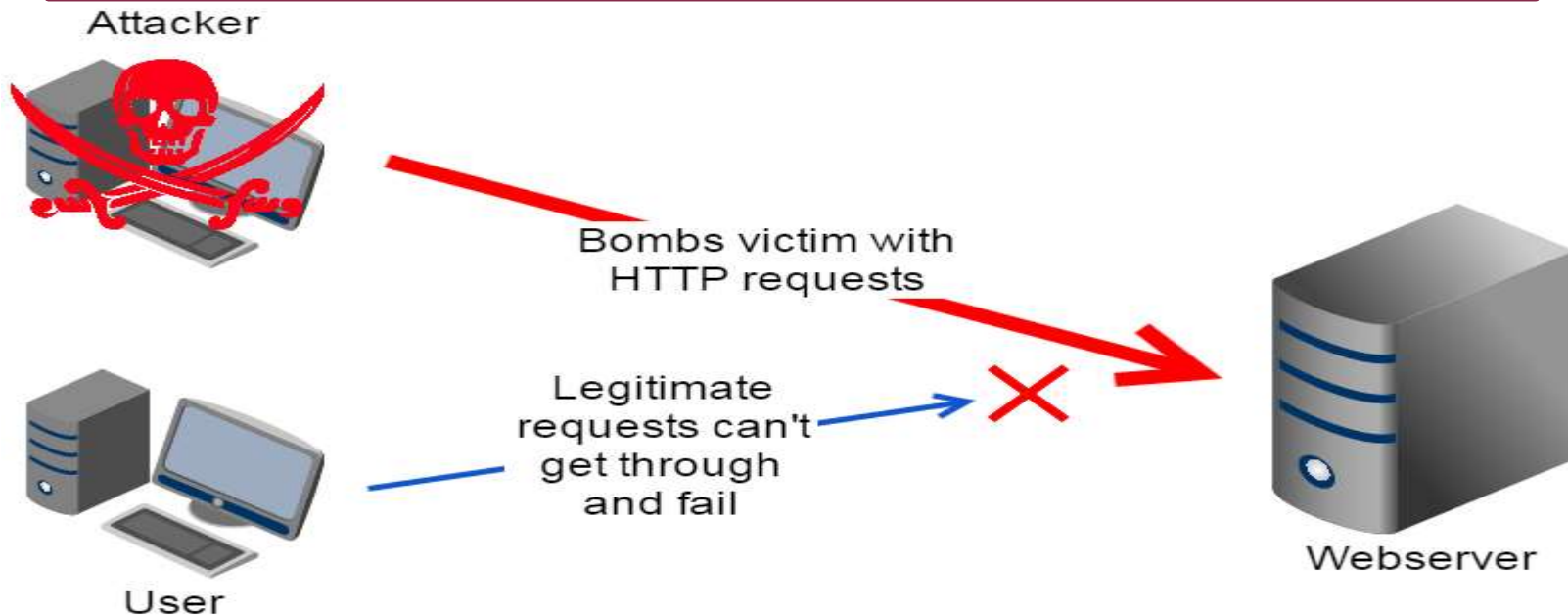
OK

VIRUS, WORMS AND TROJAN ATTACK

TROJAN ATTACK

- an unauthorized program which functions from inside what looks like authorized program, thereby concealing what it is actually doing.

A Trojan Horse Was Found!

There is no reason to worry, though. avast! has stopped the malware before it could enter your computer. When you click on the "Abort connection" button, the download of the dangerous file will be canceled.

File name: http://www13.plala.or.jp/setfsb/download/beta/setfsbU15a3_P5W

Malware name: Win32:Killwin-F [Trj]

Malware type: Trojan Horse

VPS version: 0634-0, 21/08/2006

Processing

Abort connection

DENIAL OF SERVICE (DOS) ATTACK

- **service attack** on a network by sending of disproportionate data to the victim's server beyond the limit that the server is capable to handle and hence resulting in server to crash.

Attacker

Bombs victim with HTTP requests

Legitimate requests can't get through and fail

Webserver

User

E-MAIL RELATED CRIMES

Email Spoofing

Email Spamming

Email Bombing

EMAIL SPOOFING

- a fraudulent email activity with intent to cheat the other party

E-mail Spoofing

Gujarat Ambuja Cement executive case is the best example of email spoofing in India where the former executive of the said company posed as a woman and generated a fake email ID through which he contacted Abu Dhabi based NRI businessman and deceived him for crores by blackmailing tactics.

EMAIL SPAMMING

- refers to sending of bulk-mails to thousands and thousands of users by an identified or unidentified source.

- Spamming results in reduction of productivity and wastage of time.

EMAIL BOMBING

- sending huge volumes of e-mails to a particular address which results in crashing of victim's e-mail account or mail servers.

- The email bomber blocks your inbox continuously with numerous identical emails.

- Two variants of bombing:
   Mass mailing
   List Linking

CONTD.

E-mail Bombing

There is a famous case relating to email bombing in which a foreigner was a resident of Shimla (India) for almost 30 years. The Shimla Housing Board launched a scheme to sell land at lower rates. The foreigner had applied under this scheme but his application was not accepted on the ground that the scheme was available for citizens of India. He decided to take revenge. Subsequently he sent thousands of emails to Shimla Housing Board and frequently kept sending huge volumes of email till their servers crashed.

SALE OF ILLEGAL ARTICLE

- sale of narcotics drugs, weapons and wild life etc.

- Websites, auction websites and bulletins boards may be used for posting such information.

PHISHING

- Sensitive information such as username, password, credit card details, account data etc. by disguising as a trustworthy entity .

- For example, your bank may send you email (which appears genuine to you) asking you to update your personal information by clicking at a specified link. As it appears genuine, you may be asked to visit a fraudulent site where all your sensitive information is acquired and subsequently used for cyber crimes and frauds.

- Punishable under Sections 66, 66A & 66D of the IT Act, 2000

INTELLECTUAL PROPERTY CRIMES

Distribution of pirated software

copyright infringement

trademarks violations etc

CASE STUDY

Satyam Infoway Ltd. vs. Sifynet Solutions (2004) is the most widely known case pertaining to **Cyber Squatting.**

WEB DEFACEMENT

- Substitution of the original homepage of a website with another page by a hacker or cracker.

The substituted page contains normally
- pornographic or
- defamatory material.

- Punishable under Sections 43, 66, 66F, 67 and 70 of the IT Act

CYBER STALKING & CYBER VANDALISM

CYBER STALKING/ONLINE HARASSMENT

- Use of internet, e-mail or other electronic communication devices to stalk (harass) or threatens another person by making harassing phone calls, leaving written messages or objects etc

CYBER VANDALISM

- It refers to damaging or destroying the data or property rather than stealing or misusing them.

CYBER LAWS

The I.T. Act, 2000 defines the terms –

- access in computer network in **section 2(a)**
- computer in **section 2(i)**
- computer network in **section (2j)**
- data in **section 2(0)**
- information in **section 2(v).**