Lecture Delivery Plan

UNIT 1: INTRODUCTION TO CYBER CRIME

Lecture -1:

1.1 .1 Introduction of Course Outcomes & Overview of the Syllabus

The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education. There're two sides to a coin. Internet also has it's own disadvantages is Cyber crime- illegal activity committed on the internet. Malicious programs, Illegal imports, Crime committed using a computer and the internet to steal data or information.

1.1.2 Defining Cybercrime:

Cybercrime is not a new phenomena. The first recorded cybercrime took place in the year 1820. In 1820, Joseph Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!

Alternative definitions for cybercrime could be given as:

- Any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution
- Any traditional crime that has acquired a new dimension or order of magnitude through the aid of a computer, and abuses that have come into being because of computers
- Any financial dishonesty that takes place in a computer environment.
- Any threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom

Another definition "Cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that target the security of computer systems and the data processed by them". Hence cybercrime can sometimes be called as computer-related crime, computer crime, E-crime, Internet crime, High-tech crime

Cybercrime specifically can be defined in number of ways • A crime committed using a computer and the internet to steal a person's identity(identity theft) or sell contraband or stalk victims or disrupt operations with malevolent programs. • Crimes completed either on or with a computer • Any illegal activity through the Internet or on the computer. • All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW.

Cybercrime refers to the act of performing a criminal act using cyberspace as communication vehicle. Two types of attacks are common: – Techno- crime : Active attack

• Techno Crime is the term used by law enforcement agencies to denote criminal activity which uses (computer) technology, not as a tool to commit the crime, but as the subject of the crime itself. Techno Crime is usually pre-meditated and results in the deletion, corruption, alteration, theft or copying of data on an organization's systems.

• Techno Criminals will usually probe their prey system for weaknesses and will almost always leave an electronic 'calling card' to ensure that their pseudonym identity is known.

Techno – vandalism: Passive attack

• Techno Vandalism is a term used to describe a hacker or cracker who breaks into a computer system with the sole intent of defacing and or destroying its contents. • Techno Vandals can deploy 'sniffers' on the Internet to locate soft (insecure) targets and then execute a range of commands using a variety of protocols towards a range of ports. If this sounds complex - it is! The best weapon against such attacks is a firewall which will hide and disguise your organization's presence on the Internet.

Cybercrime and Information Security

Lack of information security give rise to cybercrime

Cyber Security: means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Challenges for Securing Data in Business Perspective:

Cybercrime occupy an important space in information security due to their impact.

Most organizations do not incorporate the cost of the vast majority of computer security incidents into their accounting

The difficulty in attaching a quantifiable monetary value to the corporate data and yet corporate data get stolen/lost

Financial loses may not be detected by the victimized organization in case of Insider attacks : such as leaking customer data

Lecture -2:

1.2.1 Who are Cybercriminals?

Cyber Criminals are those who conduct acts such as: – Credit card fraud – Cyber stalking – Defaming another online – Gaining unauthorized access to computer systems – Ignoring copyrights – Software licensing and trademark protection – Overriding encryption to make illegal copies – Software piracy – Stealing another's identity to perform criminal acts

Categorization of Cybercriminals

Type 1: Cybercriminals- hungry for recognition – Hobby Hackers :A person who enjoys exploring the limits of what is possible, in a spirit of playful cleverness. May modify hardware/ software – IT professional(social engineering)
Ethical hacker – Politically motivated hackers : Promotes the objectives of individuals, groups or nations supporting a variety of causes such as : Anti globalization, transnational conflicts and protest Terrorist organizations, Cyber terrorism: Use the internet attacks in terrorist activity
Large scale disruption of computer networks , personal computers attached to internet via viruses

Type 2: Cybercriminals- not interested in recognition – Financially motivated hackers • Make money from cyber attacks • Bots-for-hire : fraud through phishing, information theft, spam and extortion – State-sponsored hacking • Hacktivists • Extremely professional groups working for governments • Have ability to worm into the networks of the media, major corporations, defense departments

Type 3: Cybercriminals- the insiders – Disgruntled or former employees seeking revenge – Competing companies using employees to gain economic advantage through damage and/ or theft.
Motives Behind Cybercrime
Greed Desire to gain power Publicity Desire for revenge A sense of adventure Looking for thrill to access forbidden information • Destructive mindset • Desire to sell network security services

1.2.2 Classification of Cybercrimes:

Cybercrime against an individual Cybercrime against property Cybercrime against organization Cybercrime against Society Crimes emanating from Usenet newsgroup

1. ***Cybercrime against an Individual*** :
   - Electronic mail spoofing and other online frauds
   - Phishing, spear phishing
   - Spamming
   - Cyber defamation
   - Cyber stalking and harassment
   - Computer sabotage
   - Pornographic offenses
   - Password Sniffing

2.***Cybercrime against property*** • Credit card frauds • Intellectual property(IP) crimes • Internet time theft

3.***Cybercrime against Organization***

Unauthorized accessing of computer Password sniffing Denial-of-service attacks Virus attack/dissemination of viruses E-Mail bombing/mail bombs Salami attack/ Salami technique Logic bomb Trojan Horse Data diddling Industrial spying/ industrial espionage Computer network intrusions Software piracy

4.***Cybercrime against Society*** • Forgery • Cyber terrorism • Web jacking

Lecture -3:

1.3.1 A Global Perspective on Cyber Crime

With the rapid development of computer technology and internet over the years, the problem of cyber crime has assumed gigantic proportions and emerged as a global issue. It has created an entirely new set of problems for law enforcement agencies all over the world. It has equally become cause of serious concern for the legal fraternity to find effective ways and means to combat cyber criminality because of its worldwide devastating effect.

(Book Ref. Nina Godbole/Sunit Belapure)

- In Australia, cybercrime has a narrow statutory meaning as used in the *Cyber Crime Act* 2001, which details offenses against computer data and systems.
- In the Council of Europe's (CoE's) *Cyber Crime Treaty*, cybercrime is used as an umbrella term to refer to an array of criminal activity including offenses against computer data and systems, computer-related offenses, content offenses and copyright offenses.
- Recently, there have been a number of significant developments such as

1. August 4, 2006 Announcement: The US Senate ratifies CoE Convention on Cyber Crime.
2. In August 18, 2006, there was a news article published "ISPs Wary About 'Drastic Obligations' on Web Site Blocking."
3. CoE Cyber Crime Convention (1997–2001) was the first international treaty seeking to address Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.

Cybercrime and the Extended Enterprise

- It is the responsibility of each user to become aware of the threats as well as the opportunities that "connectivity" and "mobility" presents them with.
- **Extended enterprise** - represents the concept that a company is made up not just of its employees, its board members and executives, but also its business partners, its suppliers and even its customers (Fig. 5).

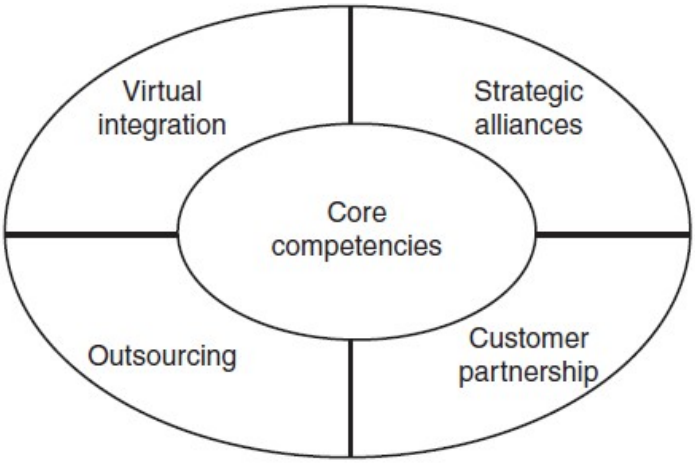


Figure 5 | Extended enterprise.

1.3.2 Cyber Crime Era: Survival Mantra for the Netizens

Cyber Crime Era:

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them.

Survival Mantra for the Netizens

- Netizen is someone who spends considerable time online and also has a considerable presence online (through websites about the person, through his/her active blog contribution and/or also his/her participation in the online chat rooms).
- The 5P Netizen mantra for online security is: (a) Precaution, (b) prevention, (c) Protection, (d) Preservation and (e) Perseverance**.**

For ensuring cyber safety, the motto for the "Netizen" should be "Stranger is Danger!"

Cyber Security: Most Challenging:

Indeed, Cyber Security has become one of the most challenging tasks in computer science field; and it is expected that the number and sophistication of cyber attacks will grow continually and exponentially.

Lecture – 4

1.4.1. Cyber Offences: How Criminals Plan the Attacks

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.

2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.

3. Launching an attack (gaining and maintaining the system access).

Reconnaissance:

"Reconnaissance" is *an act of reconnoitering – explore, often with the goal of finding something or somebody* (*especially to gain information about an enemy or potential enemy*).

Reconnaissance begins with "*Footprinting*" – this is the preparation toward pre-attack phase

- involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.

Passive Attacks

- A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge.
- It is usually done using Internet searches or by Googling an individual or company to gain information.

Active Attacks

- An active attack involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase.
- It involves the risk of detection and is also called "*Rattling the doorknobs*"or "*Active reconnaissance*."
- Active reconnaissance can provide confirmation to an attacker about security measures in place.

Scanning and Scrutinizing Gathered Information

The objectives of scanning are:

1. Port scanning: Identify open/close ports and services.

2. Network scanning: Understand IP Addresses and related information about the computer network systems.

3. Vulnerability scanning: Understand the existing weaknesses in the system.

Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password;
2. exploit the privileges;
3. execute the malicious commands/applications;
4. hide the files (if required);
5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

Lecture – 5

1.5.1 Social Engineering

- It is the "technique to influence" and "persuasion to deceive" people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers' word, rather than exploiting computer security holes.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- The sign of truly successful social engineers is that they receive information without any suspicion.

Classification of Social Engineering:

1. *Human-Based Social Engineering*
Human-based social engineering refers to person-to-person interaction to get the required/desired information.

2. *Computer-Based Social Engineering*
Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.

1.5.2 Cyber Stalking

- Cyber-stalking, simply put, is online stalking.
- In other words, the use of the internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization.
- "Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

Ways of Stalking

- False accusations,
- Monitoring,
- Threats,
- Posting personal informations
- Continuously following the victim in online

Motives Behind Stalking

- To control the victims
- Threats and other threats of violence

- Posting of women's personal information
- Harassment
- Revenge & Hate

Types of Stalking

- E-mail talking: Direct communication through email.
- Internet Stalking: Global communication through the Internet.
- Computer Stalking : Unauthorised control of an other person's computer.

How Stalking Works?

1. Personal information gathering about the victim
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.
5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

Way to Prevent Stalking

- Maintain vigilance over physical access to your computer and other Web enabled devices like cell phones
- Cyber-stalkers use software and hardware devices sometimes attached to the back of your PC without you even knowing to monitor their victims.
- Make sure you always log out of your computer programs when you step away from the computer and use a screensaver with a password.
- Make sure to practice good password management and security. Never share your passwords with others, and be sure to change your passwords frequently.

Lecture -6

1.6.1 Cyber Cafe and Cyber Crime

- Cybercriminals prefer cybercafes to carry out their activities.
- The criminals tend to identify one particular personal computer PC to prepare it for their use.
- Cybercriminals will visit these cafes at a particular time and on the prescribed frequency, maybe alternate day or twice a week.
- Pirated software(s) such as OS, browser, office automation software(s) (e.g., Microsoft Office) are installed in all the computers.
- Antivirus software is found to be not updated to the latest patch and/or antivirus signature
- Several cybercafes had installed the software called "Deep Freeze" for protecting the computers from prospective malware attacks.
- Annual maintenance contract (AMC) found to be not in a place for servicing the computers; hence, hard disks for all the computers are not formatted unless the computer is down.
- Not having the AMC is a risk from cybercrime perspective because a cybercriminal can install a Malicious Code ona computer and conduct criminal activities without any interruption.
- Cybercafe owners have very less awareness about IT Security and IT Governance.
- Cybercafe association or State Police (cyber cell wing) do not seem to conduct periodic visits to cybercafes
- Individual should take care while accessing computers in public places, that is, accessing the Internet in public places such as hotels, libraries and holiday resorts.
- Moreover, one should not forget that whatever is applicable for cybercafes (i.e., from information security perspective) is also true in the case of all other all public places where the Internet is made available.

1.6.2 Safety and Security @ Cyber Café

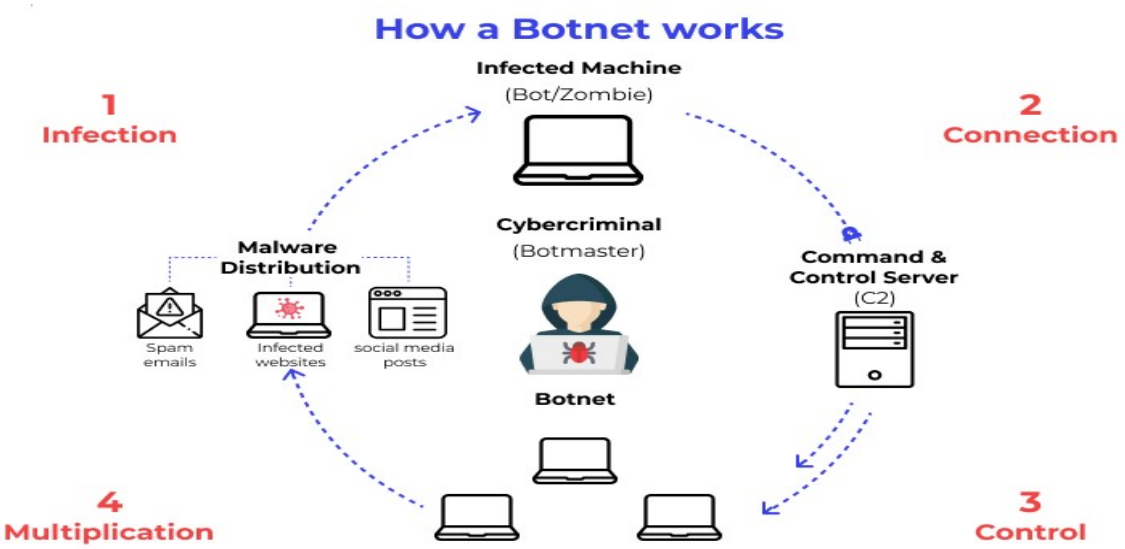
- Always logout: While checking E-Mails or logging into chatting services such as instant messaging or using any other service that requires a username and a password, always click "logout" or sign out" before leaving the system.
- Simply closing the browser window is not enough, because if somebody uses the same service after you then one can get an easy access to your account. – However, do not save your login information through options that allow automatic login. Disable such options before logon.
- Stay with the computer: While surfing/browsing, one should not leave the system unattended for any period of time. – If one has to go out, logout and close all browser windows.

- Clear history and temporary files: Internet Explorer saves pages that you have visited in the history folder and in temporary Internet files.
- Your passwords may also be stored in the browser if that option has been enabled on the computer that you have used.
- Therefore, before you begin browsing, do the following in case of the browser Internet Explorer: Go to Tools →Internet options → click the Content tab → click Auto Complete. If the checkboxes for passwords are selected, deselect them.
- Click OK twice. After you have finished browsing, you should clear the history and temporary Internet files folders.
- For this, go to Tools →Internet options again → click the General tab → go to Temporary Internet Files →click Delete Files and then click Delete Cookies. Then, under history, click clear history. Wait for the process to finish before leaving the computer.
- Be alert: One should have to stay alert and aware of the surroundings while using a public computer. Snooping over the shoulder is an easy way of getting your username and password.
- Avoid online financial transactions: Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card or bank account details. In case of urgency one has to do it; however, one should take the precaution of changing all the passwords as soon as possible. One should change the passwords using a more trusted computer, such as at home and/or in office.
- Change password
- Virtual keyboard: Nowadays almost every bank has provided the virtual keyboard on their website.
- Security warnings: One should take utmost care while accessing the websites of any banks/financial institution.

Lecture – 7

1.7.1 Botnets: The Fuel for Cybercrime

- A botnet is a collection of independent computers that have each been hacked by a cyber criminal who uses them as a group to carry out many malicious attacks over the Internet.
- In a botnet, each computer is remotely controlled by a hacker.
- A botnet is a collection of independent computers that have each been hacked by a cyber criminal who uses them as a group to carry out many malicious attacks over the Internet.
- In a botnet, each computer is remotely controlled by a hacker.
- Botnet is a term used for collection of software robots, or Bots, that run autonomously and automatically.
- The term is often associated with malicious software but can also refer to the network of computers using distributed computing software.
- In simple terms, a Bot is simply an automated computer.
- One can gain the control of your computer by infecting them with a virus or other Malicious Code that gives the access.
- A computer system maybe a part of a Botnet even though it appears to be operating normally.



- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.
- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- "Zombie networks" have become of income for entire groups of cybercriminals.

- The invariably low cost of maintaining a Botnet and the ever diminishing degree of knowledge require to manage one are conducive to the growth in popularity and, consequently, the number of Botnets.

Way of Safety:

One can reduce the chances of becoming part of a Bot by limiting access into the system. Leaving your Internet connection ON and unprotected is just like leaving the front door of the house wide open.

1. Use antivirus and anti-Spyware software and keep it up-to-date:

It is important to remove and/or quarantine the viruses.

The settings of these softwares should be done during the installations so that these softwares get updated automatically on a daily basis.

2. Set the OS to download and install security patches automatically:

OS companies issue the security patches for flaws that are found in these systems.

3. Use a firewall to protect the system, from hacking attacks while it is connected on the Internet:

A firewall is a software and/or hardware that is designed to block unauthorized access while permitting authorized communications.

is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.

A firewall is different from antivirus protection. Antivirus software scans incoming communications and files for troublesome viruses vis-a-vis properly configured firewall that helps to block all incoming communications from unauthorized sources.

4. Disconnect from the Internet. when you are away from your computer: Attackers cannot get into the system when the system is disconnected from the Internet.

Firewall, antivirus, and anti-Spyware softwares are not foolproof mechanisms to get access to the system.

5. Downloading the freeware only from websites that are known and trustworthy: It is always appealing to download free software(s) such as games, file-sharing programs, customized toolbars, etc.

However, one should remember that many free software(s) contain other software, which may include Spyware.

6. Check regularly the folders in the mail box- "sent items" or "outgoing"-for those messages, you did not send: If you do find such messages in your outbox, it is a sign that your system may have infected with Spyware, and maybe a part of a Botnet.

This is not full proof; many spammers have learned to hide their unauthorized access.

7. Take an immediate action if your system is infected: If your system is found to be infected by a virus, disconnect it from the Internet immediately.

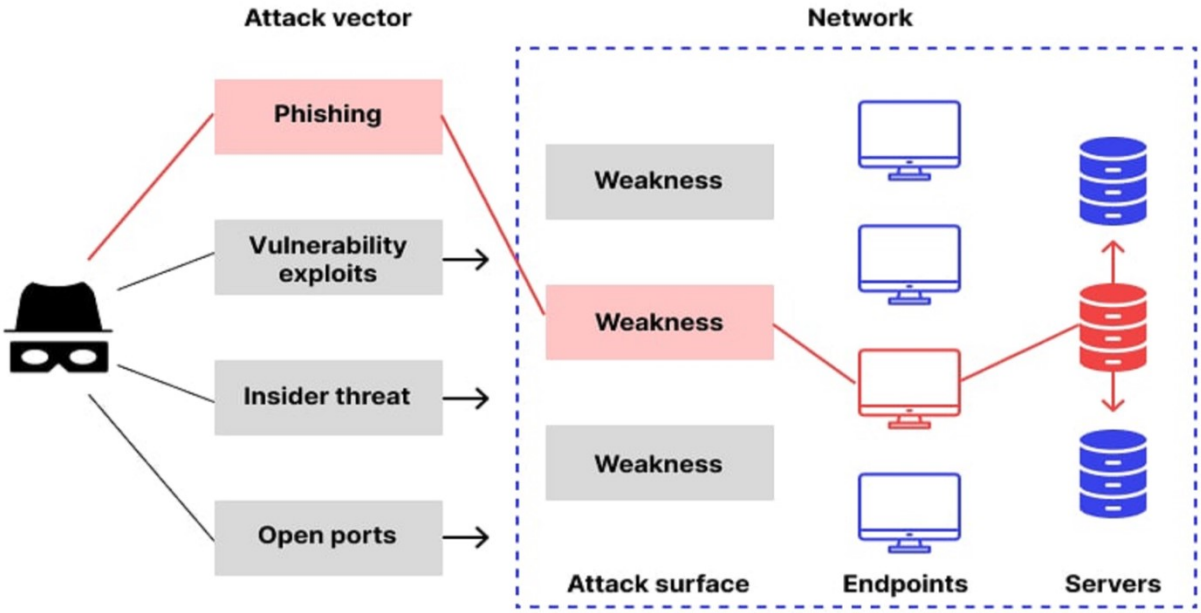
Then scan the entire system with fully updated antivirus, and anti-Spyware software. Report the unauthorized accesses to ISP and to the legal authorities.

There is a possibility that your passwords may have been compromised in such cases, so change all the passwords immediately.

Lecture -8:

1.8.1 Attack Vector

- An attack vector is a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities.
- Hackers use numerous attack vectors to launch attacks that take advantage of system weaknesses, cause a data breach, or steal login credentials.
- An attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception.
- The most common malicious payloads are viruses, Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.
    - Payload means the malicious activity that the attack performs.
    - It is the bits that get delivered to the end-user at the destination.



The attack vectors described here are how most of them are launched:

1. Attack by E-Mail
2. Attachments (and other files)
3. Attack by deception
4. Hackers
5. Heedless guests (attack by webpage)

6. Attack of the worms
7. Malicious macros
8. Foistware (sneakware)
9. Viruses

Revision of Unit -1 & Doubt Clearance