# Cyber Security

**Ms.Minal Anant Apandkar**

*Lecturer at VPM's Polytechnic, Thane*

**Abstract** – Cyber security is the form of skills, procedures and performs intended to defend networks, computers, programs and data from attack, damage or illegal access. Cyber security involves governing physical access to the hardware and also protecting against impairment that cause due to network access, data and code injection and also due to maladministration by operator. With increase in cyber-attacks day by day puts nation at higher risk which needs higher degree of cyber security. Cyber-crimes spoils people or nation's security and financial health. Hacking, child pornography, child grooming, copyright infringement are frightful issues which makes cyber security at higher priority.

**Key Words:** Security, Theft, Risks, Network attack, Information Technology Act.

## 1. INTRODUCTION

Cyber Security is the process of detecting and preventing any illegal use of laptop/computer. It comprises the process of protection against snoopers from using your private or workplace based computer resources with nasty intent or for their own gains or even for gaining any access to them accidentally. Major regions encircled in cyber security are:

### 1.1 Application Security

Application security incorporates measures taken to improve the security of an application. Different skills used to attain this are design, development, deployment, upgrade or maintenance. To achieve higher degree of application security actions can be taken such as use of application firewall which limits the execution of files or handling of data by specific installed programs and also use of router is also advantageous which prevent the IP address of an individual computer from being directly visible on internet. Also use of conventional firewalls, anti-virus programs, and spyware detection can be used to achieve application security.

### 1.2 Information Security

Information security protects information from illegal admittance to avoid identity theft and to defend discretion. Major practices used to cover this are: a) Identification, validation & approval of user, b) Cryptography.

### 1.3 Disaster Recovery

After natural disaster (flood, earthquake etc.) or cyber-attack there are chances of losing important data which is not desirable for official or personal use of computer/laptop. To avoid this disaster recovery plan is must. It is set of policies and procedures to enable the recovery.

### 1.4 Network Security

Network security comprises actions to safeguard the usability, reliability, integrity and security of the network. Effective network security aims a variety of threats and stops them from arriving or spreading on the network. Network security components contain: a) Anti-virus and anti-spyware, b) Firewall, to block unconstitutional access to your network, c) Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks, and d) Virtual Private Networks (VPNs), to provide secure remote access.

## 2. COMPUTER SECURITY RISKS

This is an occasion or action that could cause damage to or loss of computer hardware, software data information, or processing ability.

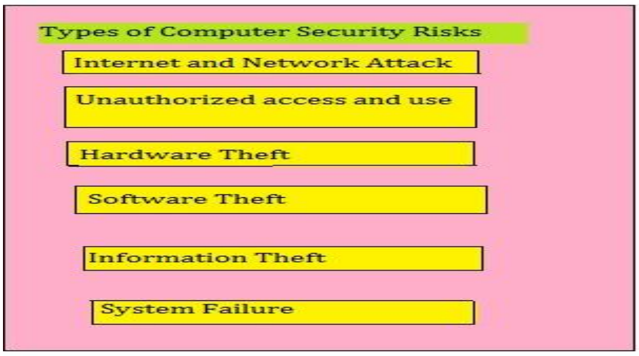
Types of Computer Security Risks
Internet and Network Attack
Unauthorized access and use
Hardware Theft
Software Theft
Information Theft
System Failure

Fig 1:-Types of Computer Security Risks

### 2.1 Internet and Network Attack

Information transmitted over network having higher security risk than information kept on office premises.

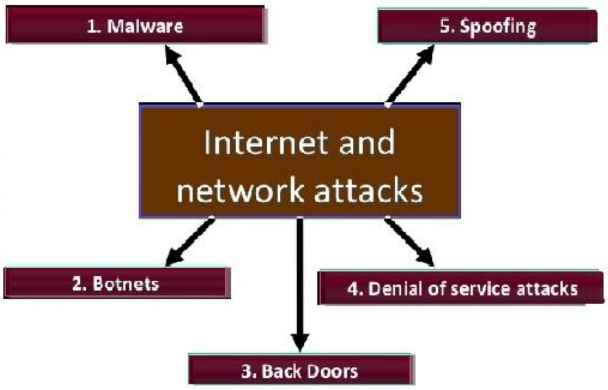

Fig -2: Internet and network attack

### 2.1 .1 Malware

Malware are program that act without operator's awareness and deliberately change the operation.

### 2.1 .2 Botnets

It's a collection of compromised computers associated to a network such as internet that are used as part of network that attacks other networks, usually for nefarious purposes.

### 2.1 .3 Back Doors

A program or set of commands in a program that allows users to sidestep security controls when retrieving a program, computer or network.

### 2.1 .4 Spoofing

It is a deceitful or nasty exercise in which communication is sent from an unfamiliar causes disguised as a source known to the receiver. Spoofing is most dominant in communication mechanisms that lack a high level of safety.

### 2.2 Unauthorized Access and Use

Unauthorized access is a use of computer or network without approval. Unauthorized use is the use of computer or its data for unapproved or possibly unlawful activities.

### 2.3 Hardware Theft

Hardware theft is the act of stealing computer equipment.

### 2.4 Software Theft

Software theft occurs when someone steal software media or intentionally erases/copies program or illegally registers and/or activates a program

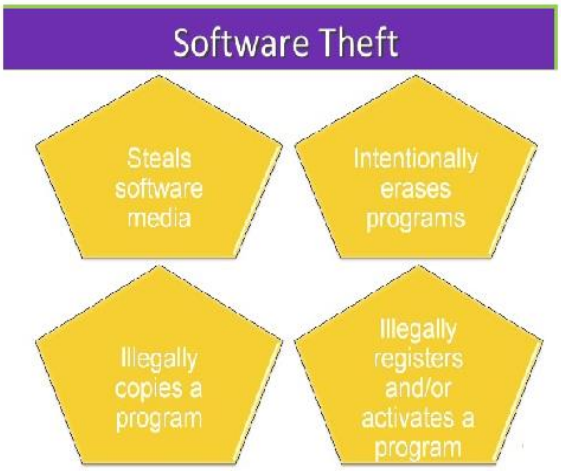
Software Theft
Steals software media
Intentionally erases programs
Illegally copies a program
Illegally registers and/or activates a program

Fig -3: Software Theft

### 2.5 Information Theft

It happens when someone steals personal or confidential information.

### 2.6 System Failure

System failure is the persistent malfunction of the computer. A variation of aspects can prime system failure, comprising aging hardware, natural disaster, electrical power problems, noise, undervoltages and over voltages errors in computer programs.

## 3. DIFFERENT ELEMENTS IN COMPUTER SECURITY

Different elements in computer security are confidentiality, integrity and availability.

### 3.1 Confidentiality

Confidentiality is the disguise of information or possessions. Also, there is a necessity to retain information undisclosed from other third parties that need to have admittance to it, so just the right people can access it.

### 3.2 Integrity

Integrity is defined as the trustworthiness of data in the systems or resources by the point of view of avoiding unauthorized and inappropriate changes.

### 3.3 Availability

Availability discusses to the ability to access data of a resource when it is preferred, as such the information has importance only if the authorized people can access at right time. Disagreeing access to data now a days has become a common attack.

## 4. APPLICATION SECURITY

Application security comprises measures taken to develop the safekeeping of an application often by finding, fixing and preventing security disclosures. Different methods used are design, development, deployment, upgrade, or maintenance. An always developing but largely reliable set of common security flaws are seen across different applications.

## 5. CYBER SECURITY POLICY

The cyber security policy is an emerging task that offers to the all-inclusive field of Information and Communication Technology (ICT) users and benefactors. It comprises –

Home operators

Small, medium, and large Enterprises

Government and non-government entities

It works as a specialist agenda that describes and escorts the events connected with the security of cyberspace. It sanctions all sectors and establishments in scheming appropriate cybersecurity procedures to encounter their necessities. The policy provides an outline to effectively protect information, information systems and networks.

It gives a thoughtful into the Government's approach and approach for security of cyber space in the country. It also plans some pointers to agree cooperative working across the public and private sectors to safeguard information and information systems. Therefore, the aim of this procedure is to create a cybersecurity framework, which leads to comprehensive actions and programs to increase the security carriage of cyberspace.

### 5.1 Information Technology Act

The Government of India endorsed The Information Technology Act with some chief purpose as to provide authorized acknowledgment for communications through electronic data interchange (EDI) and other means of electronic communication commonly referred to as electronic commerce or E-Commerce.

### 5.2 National Cyber Security Policy 2013

In India Government revealed a National Security Policy 2013 on 2 July 2013 for providing economic benefit to business for implementation of standard safety practices and methods and to empower security of information while in process handling so as to maintain privacy of resident's data and reducing financial losses with strategies as follows-

Safeguarding E-Governance services.

Forming cyber security consciousness.

Producing an assurance framework.

Creating a safeguarded framework.

Developing operative public private partnership.

Decreasing supply chain risks.

## 6. TIPS TO PREVENT CYBER-CRIMES

Keep reading the latest ways hackers create phishing scams to gain access to your personal information.

Install a firewall on computer/laptop to keep unwanted threats and attacks to a minimum.

Be careful while opening emails and clicking links. Be careful while downloading content from unsupported causes.

## 7. CONCLUSIONS

Cybercrime are the one of biggest concern which our nation is facing in 21st century. With day by day progress in technology criminals making misuse of technology, they don't rob bank or house or they even don't stole ornaments, they use mouse cursor and passwords as weapons for hacking personal or official important information which is more dangerous than any other weapon. This leads our nation as well as their resident to suffer from financial losses. To overcome these kind of issues and better use of advanced technology one has to be careful while using technology and also person or organization should have disaster or back up plan to be ready in advance if such scenario happens with them to avoid future losses. People can be make alert with crimes which are happening surrounding so that they can take necessary precautions while using advanced technology such as net banking, e-services etc.

## REFERENCES

"Handbook of Applied Cryptography" by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone.

"Cryptography and Network Security: Principles and Practice" by William Stallings

Computer and Information Security Handbook, 2nd Edition by john R.Vacca