Cyber Security – is the safe and responsible use of information and communication technology. It is not just about keeping information safe and secure but also being responsible with that information.

- As information infrastructure and Internet became bigger and more complex, it became critical to maintain systems functional and alert to security issues.

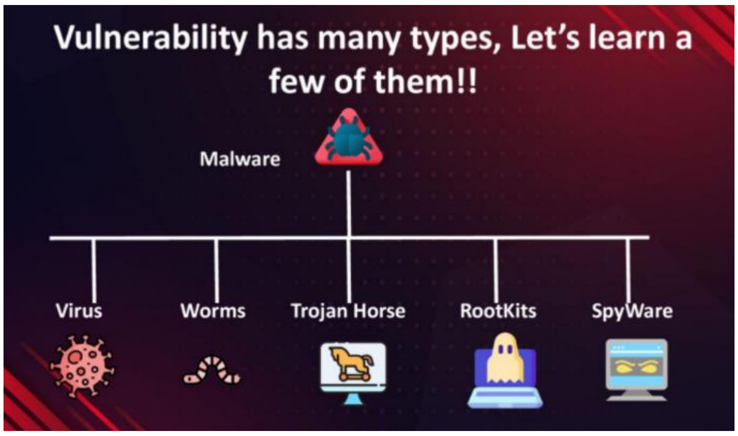
Internet - a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Vinton Cerf - Widely known as a "**Father of the Internet**," co-designer of TCP/IP protocols and basic architecture of the Internet.

Cybersecurity Vulnerability - is any weakness within an organization's information systems, internal controls, or system processes that can be exploited by cybercriminals.

- Through points of vulnerability, cyber adversaries are able to gain access to your system and collect data. With regard to your organization's overall security posture, cybersecurity vulnerabilities are extremely important to monitor as gaps in a network can lead to a full-scale breach of a system.

Types of Vulnerability



Vulnerability has many types, Let's learn a few of them!!

Malware - is a short term used for Malicious software. It is any software developed with an intention to damage hardware devices, steal data, or cause any other trouble to the user.

Virus - Mimicking the behavior of a biological virus, the computer virus spreads on contact with another system, i.e. a computer virus infects other computer systems that it comes into contact with.

- A **virus** remains dormant on a system and is activated as soon as the infected file is opened (executed) by a user.

Worm - Also, a virus needs human triggering for replication (i.e. when a user opens/executes the infected file), while a worm replicates on its own and can spread to other computers through the network.

- Some prominent examples of worms include Storm Worm, So big, MS Blast, Code Red, Nida, Morris Worm, etc.

What is saving us from all these Malwares?

As they say,

"Solution comes before Problems do",

even we have our Security Majors....

Security Major - is specifically designed for individuals interested in securing computer systems, networks, and information from cyber threats.

Types of Security Majors

- **Anti-virus**
- **Firewall**
- **Anti-Malware**

Antivirus - is a software, also known as anti-malware Initially, antivirus software was developed to detect and remove viruses only and hence the name antivirus.

Firewall - is a network security system designed to protect a trusted private network from unauthorized access or traffic originating from an untrusted outside network.

- Monitors Network Traffic
- Stops Virus Attacks
- Prevents Hacking
- Stops Spyware
- Promotes Privacy

Anti-Malware – Anti-spyware is a type of software that is designed to detect and remove unwanted spyware programs. Spyware is a type of malware that is installed on a computer without the user's knowledge in order to collect information about them.

Cyberspace - Is a complex environment consisting of interactions between people, software, and services, supported by the worldwide distribution of information and communication technology (ICT) devices and networks.

Key Features of Cyber Space

Global Connectivity - Cyberspace connects individuals, businesses, and governments across the world in a seamless digital environment.

Virtual Interactions - Users in cyberspace can interact, exchange information, and collaborate via websites, applications, and social media.

Cyber Security - Is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Core Principles of Cyber Security

Confidentiality - Keeping sensitive information private and accessible only to authorized users or entities. This involves encryption, access controls, and secure communication protocols to prevent unauthorized access.

Integrity - Ensuring that data remains accurate, complete, and trustworthy. Protection against unauthorized alterations, modifications, or corruption of data is critical for maintaining integrity.

Availability - Ensuring that systems and information are accessible and usable when needed. Measures such as redundancy, backups, and robust infrastructure help prevent and mitigate service disruptions caused by cyber-attacks or technical failures.

Importance of Cybersecurity

- Protecting personal data
- Safeguarding business information
- Ensuring online transaction security
- Preventing unauthorized access
- Mitigating the risk of cyber attacks

Cyber Attack - Is an attempt by cybercriminals, hackers or other digital adversaries to access a computer network or system, usually for the purpose of altering, stealing, destroying or exposing information.

Types of Cyber Attack

Web-based attacks - These are the attacks which occur on a website or web applications.

- Injection attacks
- Session Hijacking
- Phishing

System-based attacks - These are the attacks which are intended to compromise a computer or a computer network.

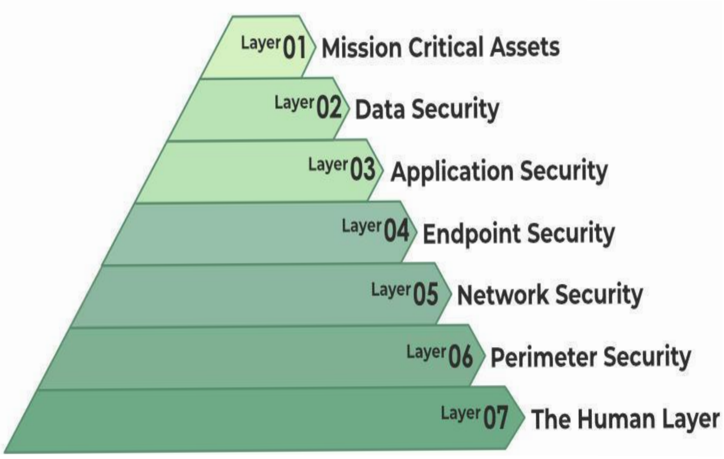
- Virus
- Worm
- Trojan horse

Cyber Criminals - Defined as an individual who engages in illegal activities using computers or digital technology, such as hacking, identity theft, online scams, malware creation, or attacks on computer systems, with the aim of achieving their goals through the exploitation of technology.

Cyber Crime - Refers to illegal activities involving computers, networks, or the internet as a tool to commit offenses.

- Cyberbullying
- Ransomware
- Identity Theft
- Cyberstalking
- Child Exploitation
- Financial Fraud
- Cyber Terrorism

7 layers of Security


Layer 01 Mission Critical Assets
Layer 02 Data Security
Layer 03 Application Security
Layer 04 Endpoint Security
Layer 05 Network Security
Layer 06 Perimeter Security
Layer 07 The Human Layer

Cyber Threat - Are security incidents or circumstances with the potential to have a negative outcome for your network or other data management systems.

- Malicious Software (Malware)
- Hacking and Intrusion
- Insider Threats

How to Protect Yourself Against Cybercrime?

- Use strong password
- Use trusted antivirus in devices
- Enable Two-Factor Authentication
- Keep your device software updated
- Use secure network
- Never open attachments in spam emails
- Software should be updated

Cyber Security Policies - Are formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It aims at protecting the public and private infrastructure from cyberattacks.

- Virus and Spyware Protection policy
- Firewall Policy
- Intrusion Prevention policy
- Application and Device Control

Information Technology Act - The Indian cyber laws are governed by the Information Technology Act, penned down back in 2000. The principal impetus of this Act is to offer reliable legal inclusiveness to eCommerce, facilitating registration of real-time records with the Government.

Penalties for Cybercrimes under IT Act, 2000

Section 43

- Deals with damage to computer systems without owner consent.
- Owner can claim full compensation for damages.

Section 66

- Addresses dishonest or fraudulent acts related to Section 43.
- Penalties include up to 3 years imprisonment or a fine up to ₹5 lakh.

Section 66B:

- Punishes fraudulently receiving stolen communication devices or computers.
- Imprisonment up to 3 years or a fine up to ₹1 lakh

Section 66C:

- Focuses on identity theft, including digital signatures, hacking passwords, and other personal identifiers.
- Penalties include 3 years imprisonment and a fine up to ₹1 lakh

Section 66D:

- Targets impersonation using computer resources.
- Punishes those who cheat through online impersonation.

Vision

To build a secure and resilient cyberspace for citizens, business, and government and also to protect anyone from intervening in user's privacy.

Mission

To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation.

OBJECTIVES

- To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
- To create an assurance framework for the design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
- To strengthen the Regulatory Framework for ensuring a SECURE CYBERSPACE ECOSYSTEM.
- To enhance and create National and Sectoral level 24X7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.