CYBER SECURITY

PROBLEM DEFINATION: Demonstration and learning of common Security threats:

- Phishing
- DoS attack
- Man in The middle attack
- Spamming
- Virus

- **What is cyber security ?**

- **Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.**

- **PHISHING :** Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need a request from their bank, for instance, or a note from someone in their company and to click a link or download an attachment.

- **DENIAL OF SERVICE ATTACK (DOS) :** A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. There are two general methods of DoS attacks: flooding services or crashing services.

- **MAN-IN-THE-MIDDLE ATTACK :** A man-in-the-middle (MitM) attack is when an attacker intercepts communications between two parties either to secretly eavesdrop or modify traffic traveling between the two. Attackers might use MitM attacks to steal login credentials or personal information, spy on the victim, or sabotage communications or corrupt data.

- **SPAMMING :** Spam refers to unsolicited bulk messages being sent through email, instant messaging or other digital communication tools. Spamming is the use of messaging systems to send an unsolicited message (spam) to large numbers of recipients for the purpose of commercial advertising, for the purpose of non-commercial proselytizing, or for any prohibited purpose (especially the fraudulent purpose of phishing).

- ## Types of cyber security

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

- **Information security** protects the integrity and privacy of data, both in storage and in transit.

- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

- ## Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

- ## Cyber safety tips - protect yourself against cyber attacks

- **Update your software and operating system:** This means you benefit from the latest security patches.
- **Use anti-virus software:** Security solutions like Kaspersky Total Security will detect and removes threats. Keep your software updated for the best level of protection.
- **Use strong passwords:** Ensure your passwords are not easily guessable.
- **Do not open email attachments from unknown senders:** These could be infected with malware.
- **Do not click on links in emails from unknown senders or unfamiliar websites:**This is a common way that malware is spread.
- **Avoid using unsecure WiFi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.

PRACTICAL OUT COMES: Learned Cyber Security Threats and Safety Measures.