ASSIGNMENT -1

Explain following terms in brief:-

1. Viruses:

Viruses are malicious software programs that attach themselves to legitimate files or software. When a user opens an infected file or runs an infected program, the virus activates and starts replicating itself, spreading to other files and potentially across a network. Viruses can have various functions, from simply causing nuisance by displaying messages or altering data to more harmful actions like corrupting files, stealing sensitive information, or granting unauthorized access to a system. Unlike some other malware, viruses often require human action to initiate their spread, such as clicking on an infected email attachment or downloading compromised software from the internet.

2. Worms:

Worms are a type of malware that can replicate and spread independently, without the need for user interaction. They take advantage of vulnerabilities in computer networks and systems to propagate rapidly. Once inside a network, a worm can move from one device to another, infecting multiple systems along the way. This can lead to network congestion, system slowdowns, or even system crashes. Worms can have a destructive impact on both individual devices and entire organizations, and they often require robust cybersecurity measures to detect and prevent their spread. It's essential to keep software and systems up to date with security patches to defend against worm attacks.

3. Phishing:

Phishing attacks involve deceptive tactics to trick individuals into revealing sensitive information or performing actions that benefit the attacker. Typically, this is done through fraudulent emails, websites, or messages that appear legitimate. Phishing emails may impersonate trusted organizations or individuals, urging recipients to click on malicious links or download infected attachments. Once the victim complies, the attacker can steal login credentials, credit card numbers, or other valuable data. Phishing is a prevalent and effective

form of cybercrime because it exploits human psychology and trust. Staying vigilant and verifying the authenticity of requests for sensitive information can help protect against phishing attacks.

4. Keyloggers:

Keyloggers are a type of malware designed to record every keystroke made on a computer or mobile device. They can operate as software programs or hardware devices. Keyloggers silently capture information like usernames, passwords, credit card details, and personal messages. Cybercriminals use this stolen data for various malicious purposes, such as identity theft, financial fraud, or unauthorized access to accounts. Protecting against keyloggers requires a combination of robust cybersecurity practices, including using reputable antivirus software, regularly updating software and operating systems, and being cautious when downloading files or visiting websites of unknown origin. Additionally, it's essential to secure physical access to your devices to prevent the installation of hardware keyloggers.

5. Trojans:

Trojans, short for "Trojan horses," are a type of malicious software that disguises itself as a legitimate or desirable program but contains hidden malicious functionality. Unlike viruses and worms, Trojans do not self-replicate. Instead, they rely on user interaction to spread. Once installed on a system, Trojans can carry out various harmful activities, such as stealing sensitive data, providing unauthorized access to the attacker, or delivering additional malware onto the infected device. Trojans often come disguised as innocuous files, like software installers or email attachments, and can be challenging to detect without robust cybersecurity tools and practices.

6. Trapdoors and Backdoors:

Trapdoors and backdoors are unauthorized methods of accessing computer systems or networks. While they serve different purposes, they share the common goal of providing secret access to a system. A trapdoor is a hidden entry point intentionally left by software developers for debugging or maintenance purposes but can be exploited by malicious actors

if not adequately secured. In contrast, a backdoor is a secret entry point inserted into a system by an attacker or malicious software to allow remote access or control. Backdoors can be used to maintain unauthorized access for spying, data theft, or launching further attacks. Detecting and closing trapdoors and backdoors are critical for maintaining system security, and it often requires thorough security audits and regular monitoring of system activity.

7. Spam:

Spam refers to unsolicited and often irrelevant or malicious messages sent via email, instant messaging, or other digital communication channels. It includes advertisements, phishing attempts, and other unwanted content. Spam can be a nuisance, overwhelming inboxes and wasting time, but it can also carry cybersecurity risks. Some spam messages contain malware or links to malicious websites that can infect devices or steal sensitive information when clicked. To combat spam, email providers and organizations use spam filters and employ various techniques to identify and block unwanted messages. Users can also play a role in reducing spam by being cautious about sharing their email addresses and reporting suspicious messages.