

Cyber security

Research Methodology in Computer Science

Dr. [Mohammed Anbar](#)

Prepared by: [Tahani Hussain](#)

1- Definition:

Cybersecurity is the protection of Internet-connected systems such as hardware, software, and data from cyber threats. This practice is used by individuals and organizations to protect against unauthorized access to data centers and other computerized systems

1 Introduction:

A strong cybersecurity strategy can provide a good security posture against malicious attacks designed to access, modify, delete, destroy or extort an organizations or user's systems and sensitive data.

Cybersecurity is also useful in preventing attacks that aim to disrupt or disrupt system or device operations.

With the increasing number of users, devices and software in modern organizations, along with an increasing deluge of data much of which is sensitive or confidential. The importance of cybersecurity continues to grow. The increasing size and sophistication of cyber attackers and attack techniques further complicates the problem.

A cybersecurity attack can lead to everything from identity theft to extortion attempts and loss of important data like family photos. Everyone believes on critical infrastructure like power plants, hospitals and financial services companies. Securing these and other organizations is essential to keeping our community functioning.

2. Category:

Cybersecurity can be divided into several common categories:

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

Application security focuses on keeping software and hardware free from threats. A compromised application can provide access to data it is designed to protect. Successful security begins at the design stage, long before the software or hardware is deployed.

Information security protects integrity and privacy of data

Operational security includes the processes and decisions to handle and protect data assets. The permissions that users have when accessing a network and the procedures that determine how and where data can be stored or shared all fall under this umbrella.

Disaster recovery and business continuity can define how an organization responds to a cybersecurity incident or any other event that causes a loss of operations or data.

Disaster recovery policies dictate how an organization restores its operations and information to return to the same operational capability as before the event. Business continuity is the plan that an organization comes back to while trying to operate without certain resources.

End-user education addresses the most unpredictable factor in cybersecurity: people.

Anyone has the ability to introduce a virus into a secure system by not following good security practices. Teaching users to delete suspicious email attachments, not to plug in unidentified USB drives, and many other important lessons are vital to the security of any organization

3- Types of cyber threats

The threats that cybersecurity addresses are threefold:

1. Cybercrime involves individual actors or groups targeting systems for financial gain or disruption.
2. Online cyberattacks often involve politically motivated information gathering.
3. Cyber terrorism aims to undermine electronic systems to cause panic or fear.

How do malicious actors take control of computer systems? Here are some common methods used to compromise cybersecurity:

Malware

Malware means malicious software. One of the most common cyber threats, malware is software created by a cybercriminal or hacker to disable or damage a legitimate user's computer.

Malware is always spread through a legitimate-looking spam email attachment or download, and may be used by cybercriminals to make money or in politically motivated cyberattacks.

There are different types of malware, including:

Virus: A self-replicating program that attaches itself to file cleaning and spreads throughout the computer system, infecting files with malicious code.

Trojans: A type of malware that masquerades as legitimate software. Cybercriminals trick users into loading Trojans onto their computers where they damage or collect data.

Spyware: Software that secretly records what a user does, so cybercriminals can take advantage of this information. For example, spyware can capture credit card details.

Ransomware: Malware that seizes a user's files and data, threatening to erase them unless a ransom is paid.

Adware: that can be used to spread malware.

Botnets: Networks of computers infected with malware that cybercriminals use to perform online tasks without user permission.

Phishing

Phishing is the training of sending fraudulent emails that resemble emails from reputable sources. The goal is to steal sensitive data such as credit card numbers and login information.

It is the common type of cyber-attack. You can help protect yourself with education or a technical solution that filters malicious emails.

Ransomware

Ransomware is a type of malware. It is designed to extort money by blocking access to files or computer system until the ransom is paid. Paying the ransom does not guarantee file recovery or system restore.

Denial of service attack

Denial of Service (DOS) attacks are designed to make a device or network resource unavailable to its intended users. Attackers can deny service to individual victims, for example by intentionally entering the wrong password enough consecutive times to cause an error in the victim's account.

This version was published simultaneously. While a network attack can be blocked from an IP address, the defense can prevent a large number of attacks. These attacks can manifest themselves in reflection and amplification attacks, where these connections in turn lead to postal actions.

Plagiarism

Main article: Spoofing attack

Spoofing is the act of masquerading as a valid entity by falsifying data (such as an IP or user address), in order to gain access to information or resources that a person is otherwise not authorized to have.

There are a lot of types of plagiarism, including:

- Email spoofing, where the attacker forges the sending address (from, or source) of an email.
- IP spoofing, where an attacker changes the source IP address in a network packet to hide his identity or impersonate another computing system.
- MAC spoofing, where the attacker modifies the network interface's Media Control (MAC) address to hide their identity, or pose as someone else.