**Module 1 CS- Introduction**

1. **what is meaning of cyber security ?**

Cybersecurity means protecting computers, servers, networks, and data from unauthorized access, attacks, or damage.

In simple words:  
Cybersecurity is the practice of keeping your digital devices and information safe from hackers and other online threats.

It helps to:

* Prevent data theft (like passwords or personal info)
* Stop viruses and malware
* Protect online privacy
* Keep systems running safely and smoothly

2] what are the main objectives of cyber security?

The **main objectives of cybersecurity** are often remembered using the **CIA Triad**, which stands for:

1. **Confidentiality**
   * Keep information private and accessible only to authorized people.
   * Example: Protecting passwords or personal data.
2. **Integrity**
   * Ensure data is accurate and not changed or tampered with.
   * Example: Preventing unauthorized edits to files or records.
3. **Availability**
   * Ensure systems and data are available when needed.
   * Example: Making sure websites or apps are up and running without interruptions.

Other important objectives include:

1. **Authentication**
   * Verify the identity of users or systems before giving access.
   * Example: Logging in with a username and password.
2. **Non-repudiation**
   * Ensure that someone cannot deny their actions (like sending a message or making a transaction).
   * Example: Using digital signatures.

3] What is offensive and defensive in cyber security?

**Defensive Cybersecurity**

**Goal:** **Protect systems and data** from attacks.

* Focuses on prevention, detection, and response.
* Builds firewalls, intrusion detection systems (IDS), antivirus software, etc.
* Example activities:
  + Monitoring network traffic
  + Patching vulnerabilities
  + Responding to incidents

*Think of it like building a security system to stop burglars.*

**Offensive Cybersecurity**

**Goal:** **Find and exploit weaknesses** before attackers do.

* Often used ethically in **penetration testing** or **red teaming**.
* Helps improve defenses by simulating real attacks.
* Example activities:
  + Ethical hacking
  + Exploiting system vulnerabilities
  + Social engineering tests

*Think of it like hiring a hacker to test how secure your system is.*

4] what is cyberspace and low ?

**Cyberspace** refers to the **virtual environment** of the internet and computer networks where digital communication and data exchange happen.

* It's not a physical place but a digital space.
* Includes websites, social media, emails, cloud storage, etc.
* Example: When you chat online, watch videos, or send emails — you're using cyberspace.

*In simple words: Cyberspace is the world of computers and the internet where people interact digitally.*

**What is Cyber Law? *(You may have meant “law”)***

**Cyber Law** refers to the **legal rules and regulations** that deal with crimes and activities on the internet or digital platforms.

* It helps protect users from online crimes like hacking, identity theft, and cyberbullying.
* It also covers data protection, online transactions, and intellectual property.

*In simple words: Cyber law is the law that keeps the internet and digital world safe and fair.*

**5. What is Cyber Welfare?**

**Cyber welfare** refers to ensuring the **safe, fair, and responsible use of technology and the internet** to protect individuals and society.

* Focuses on **digital safety, privacy, and awareness**.
* Promotes **online well-being**, like protecting children from cyberbullying or spreading awareness about safe internet use.

*In simple words: Cyber welfare is about taking care of people’s safety and rights in the digital world.*

**6. Types of Hackers**

Hackers are usually categorized by their **intentions**:

| **Type** | **Hat Color** | **Purpose** |
| --- | --- | --- |
| **White Hat** | White | Ethical hackers who help improve security legally. |
| **Black Hat** | Black | Malicious hackers who break into systems illegally. |
| **Grey Hat** | Grey | Hackers who may break rules but don’t harm systems. |
| **Red Hat** | Red | Fight black hat hackers aggressively (like vigilantes). |
| **Blue Hat** | Blue | Test software for bugs before release (external testers). |
| **Green Hat** | Green | New/learning hackers trying to gain skills. |

**7. What is the full form of SOC in Cybersecurity?**

**SOC** stands for **Security Operations Center**.

* It's a team or department that **monitors and protects** an organization’s IT systems.
* They **detect, analyze, and respond** to cybersecurity threats in real time.

*Think of it as a control room for digital security.*

**8. What are the Challenges of Cybersecurity?**

Some of the main **challenges** in cybersecurity include:

1. **Increasing Cyber Threats** – More hackers, viruses, and malware.
2. **Lack of Awareness** – Many users don’t follow basic security practices.
3. **Advanced Hacking Tools** – Attackers use AI and advanced tools.
4. **Shortage of Skilled Professionals** – Not enough trained cybersecurity experts.
5. **Weak Passwords** – Users often use easy or reused passwords.
6. **Mobile and IoT Devices** – More devices mean more risk.
7. **Data Privacy Issues** – Keeping personal and sensitive data safe is harder.
8. **Zero-Day Attacks** – New, unknown threats with no fix available.