Types of Cyber Security:

Every organization's assets are the combinations of a variety of different systems. These systems have a strong cyber security posture that requires coordinated efforts across all of its systems. Therefore, we can categorize cyber security in the following sub-domains:

- **Network Security: It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.**
- **Application Security: It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modeling, etc., before a program or device is deployed.**
- **Information or Data Security: It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.**
- **Identity management: It deals with the procedure for determining the level of access that each individual has within an organization.**
- **Operational Security: It involves processing and making decisions on handling and securing data assets.**
- **Mobile Security: It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.**
- **Cloud Security: It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.**
- **Disaster Recovery and Business Continuity Planning: It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.**
- **User Education: It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.**