1. **Describe the goals of cybersecurity.**

Answer:

The process of protecting sensitive data from attack, destruction, or unauthorized access on the internet and on devices is known as cybersecurity. In order to safeguard data, networks, and devices against cyberattacks, a risk-free and secure environment is what cyber security aims to deliver.

2. **Discuss how cyberattacks profit financially from their crimes.**

Answer:

Cyber-attacks on companies are frequently planned and driven by financial gain. However, additional reasons could be:

- using hacktivism, for example, to make a social or political point
- spying on rivals in order to gain an unfair advantage
- intellectual difficulty, such as "white hat" hacking

3. **Discuss how to protect yourself against cyber risks.**

Answer:

Recognizing the risk

To secure anything, you must be aware of what it is that you are securing. For example, it is difficult, if not impossible, to secure an environment if you are unaware of what that environment is.

Therefore, in order to protect yourself, you must be aware of the assets you have, including both those in digital and related physical formats, as well as what it is that you wish to protect. They might or might not be concentrated in one place. In fact, some or perhaps all of them might be in places that are inaccessible to you. Basic elements of protection for most individuals include

- Perimeter defense
- Firewall//router
- Your physical computer(s) and any other endpoints
- Backups

4. **Discuss why physical security is an important part of cybersecurity.**

Answer:

Physical security refers to preventing unwanted physical access, whether it comes from a person or from the outside world. Physical security includes things like locking a computer in a server closet at work to stop anyone from messing with it. The purpose of physical security is to create a secure environment for an individual, family, or organization's assets and personnel. To ensure that digital systems and data are not put at danger as a result of how they are physically housed is to practice cybersecurity.

5. **Describe the security risks in working remotely.**

Answer:

Network Security Concerns

A major cybersecurity concern with working remotely involves the networks from which employees access sensitive data. If those networks aren’t properly secured, someone may steal sensitive information and malware or a hacker compromise some user’s device and leapfrog from it to other corporate device or network.

6. **How would you securing data associated with your user accounts?**

Answer:

When you use social media, bank online, purchase online, use social media, or even just browse the web, you give the parties with whom you engage all kinds of information. You get authority over sizable amounts of personal information that the party retains about you when you open and maintain an account with a bank, shop, social media service, or other online party.

7. **How could you protect yourself and your loved ones from social engineering attacks?**

Answer:

Social engineering can be avoided with general **cyber hygiene.** A broad commitment to excellent cybergenic might also lessen your vulnerability to social engineering. Your data on the machine may remain safe even if criminals socially engineer their way into your child account if, as was frequently the case during the COVID-19 pandemic, your children have access to your computer but you encrypt all your data, have a separate login, and don't give them administrator access.