**Cybersecurity: Understanding the Hype and Future Potential**

Cybersecurity definition:

Cybersecurity is a method of protecting an application, system and networks form the cyber-attacks. Cyber-attack is defined as an assault where the criminals destroy and access sensitive information such as illegally accessing someone’s bank account and adjuring money from the victim via ransomware.

Common Cybersecurity Threats:

1. Malware Attack: This attack is a very common attack where the victim is convinced to download a file which contains malware. Once the malware is installed, all confidential data are sent to the attacker and penetrating to other loopholes in the system. Some common malwares are ransomware, wiper malware, trojan virus etc.
2. Social Engineering Attacks: This is a method of manipulating the victim psychologically so that they perform the desirable activity for an attacker. Some common social engineering attacks are phishing, malvertising, pretexting etc.
3. Distributed denial of service (DDoS): Attack uses multiple machines operating in concert to attack a network or site, and these attacks cause so much extra network traffic that it is difficult for legitimate traffic to reach your site while blocking the forged attacking packets. Attacker may use your computer to attack another computer, by taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a web site or send spam to particular email addresses.

The hype of Cybersecurity today:

Due to the rise of cyber-attacks in recent years cybersecurity has become an important field that should me explored more. As the technology is advancing and Internet is becoming an important part of our lives cybercriminals try to breach data and infiltrate networks in order to steal important information. Though antivirus and firewalls are a safety tool against malwares but as the technology advances the threats constantly increases.

The cybersecurity professionals are highly responsible for designing, implementing and also monitoring security measures to protect the system from malicious attacks. A modern cybersecurity infrastructure is which can check security of network, IoT, cloud, application, endpoint and mobile is becoming very necessary.

Future of cybersecurity:

Cybersecurity field itself has a great potential in the near future due to the automation of all machineries and work via internet. The future cybersecurity potential is constantly expanding and evolving.

The professionals in this field needs to be up-to-date about the attacks so that they can protect people from cybercrime and malicious activities. As the digital world is expanding, cybersecurity is becoming an integral part of our life.

Revenue in cybersecurity market is estimated to reach US$166.20 billion in 2023. The revenue is expected to grow at an annual rate of 10.48% resulting in the market volume of US$273.60 billion by 2028.

Everyday new threats are emerging and we need to secure our systems so that we don’t fall as the victims. Cybersecurity has a large scope in future and needs to be explored more. It will play a major part in the IT industry for years