Cyber Security Threats and Mitigation

Types of Cyber Threats:

1. **Phishing:** Phishing attacks are one of the most common types of cyber threats, affecting both individuals and businesses. These attacks usually involve an email or message that appears to be from a legitimate source, such as a bank, social media platform, or an online retailer. The email will often ask the recipient to provide personal information, such as login credentials or credit card details, by clicking on a link or downloading an attachment. To mitigate the risk of phishing attacks, users should be cautious of unsolicited emails or messages and verify the sender's identity before clicking on any links or downloading any attachments.

2. **Malware:** Malware is any software that is designed to harm or disrupt computer systems. Examples of malware include viruses, worms, trojans, and ransomware. These malicious programs can cause a wide range of problems, from deleting important files to stealing sensitive information. To prevent malware attacks, individuals and businesses should install and maintain up-to-date antivirus software, regularly scan their systems for malware, and avoid downloading or opening files from untrusted sources.
3. **Denial-of-Service (DoS) Attacks:** A DoS attack is intended to disrupt normal computer system operations by overwhelming the target with traffic or requests. These attacks can result in system downtime, network outages, or data loss. To mitigate the risk of DoS attacks, businesses should ensure that their network infrastructure can handle high

volumes of traffic, implement firewalls and other network security measures, and monitor their systems for unusual traffic patterns.

Mitigation Techniques:

1. **Firewalls:** Firewalls are network security devices that monitor incoming and outgoing traffic, based on predefined rules. Firewalls can be hardware or software-based and can help to prevent unauthorised access to computer systems and networks. Firewalls can be configured to block traffic from specific IP addresses, ports, or applications, reducing the risk of cyber attacks.
2. **Antivirus Software:** Antivirus software is designed to detect and remove malware from computer systems. Antivirus software can scan files, emails, and network traffic for malicious code, and prevent malware from infecting a system. To be effective, antivirus software must be updated regularly, as new malware threats are discovered and released.
3. **Intrusion Detection Systems (IDS):** IDSs are network security devices that monitor network traffic for signs of suspicious activity. IDSs can detect attempts to exploit vulnerabilities in computer systems, as well as unauthorised access attempts. IDSs can alert security personnel to potential cyber threats, enabling them to take appropriate action to prevent an attack.
4. **Employee Training:** Employee training is essential for preventing cyber attacks. Cyber security awareness training can help employees to understand the risks associated with cyber threats, such as phishing and malware, and how to recognise and report suspicious activity. Training can also help employees to adopt good cyber security practices, such as using strong passwords, avoiding public Wi-Fi networks, and backing up data regularly.

In conclusion, cyber security threats are a major concern for individuals and businesses alike. By understanding the types of cyber threats and implementing effective mitigation techniques, such as firewalls, antivirus software, IDSs, and employee training, businesses can reduce the risk of cyber attacks and protect their digital assets.