**Cyber Security Threats**

**What is Cyber Security?**

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security

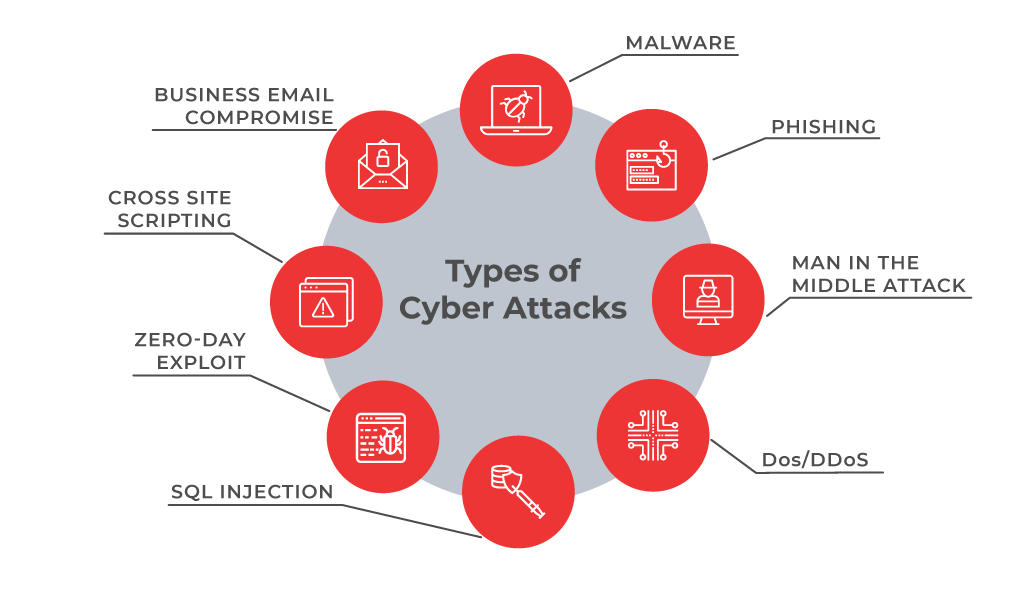
**What are Cyber Threats?**

A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information.

**Why is it necessary to protect from cyber threats?**

Cyber threats are a big deal. Cyber-attacks can cause electrical blackouts, failure of military equipment and breaches of national security secrets. They can result in the theft of valuable, sensitive data like medical records. They can disrupt phone and computer networks or paralyze systems, making data unavailable. It’s not an exaggeration to say that cyber threats may affect the functioning of life as we know it.

**Types of Cyber security Threats**



### **Malware**

### Malware attacks are the most common type of cyberattack**.** Malware is malicious software that is designed to gain unauthorized access to data or to cause damage to computers and computer systems.

1. **Advanced persistent Threats**

Advanced persistent threats, or APTs, are long-term targeted attacks that break into a network in multiple phases to avoid detection. An advanced persistent threat occurs when a malicious actor gains unauthorized access to a system or network and remains undetected for an extended time.

1. **Denial of Services**

Denial of Service attacks aims at flooding systems, networks, or servers with massive traffic, thereby making the system unable to fulfill legitimate requests. Attacks can also use several infected devices to launch an attack on the target system. This is known as a Distributed Denial of Service (DDoS) attack.

1. **Phishing**

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine. Phishing is an increasingly common cyber threat.

1. **SQL Injection:**

A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box

1. **Man in the Middle Attack**

A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.

1. **Zero-day Exploit**

A zero-day attack occurs when software or hardware vulnerability is announced, and the cybercriminals exploit the vulnerability before a patch or solution is implemented

1. **DNS Attack**

A DNS attack is a cyberattack in which cybercriminals exploit vulnerabilities in the Domain Name System. The attackers leverage the DNS vulnerabilities to divert site visitors to malicious pages (DNS Hijacking) and exfiltrate data from compromised systems (DNS Tunneling).

1. **Ransomware**

Ransomware is one type of malicious software that cyber criminals use to gain access to sensitive information within a system, encrypt the data so that the user can’t access it, and finally demand a financial payout in exchange for that data.

1. **Password Attacks**

Cracking a password is the simplest way for hackers to gain access to their target’s accounts and databases. There are three main types of password attacks: brute force attack, which involves guessing at passwords until the hacker gets in; dictionary attack, which uses a program to try different combinations of dictionary words; and key logging, which tracks all of a user’s keystrokes including login IDs and passwords.

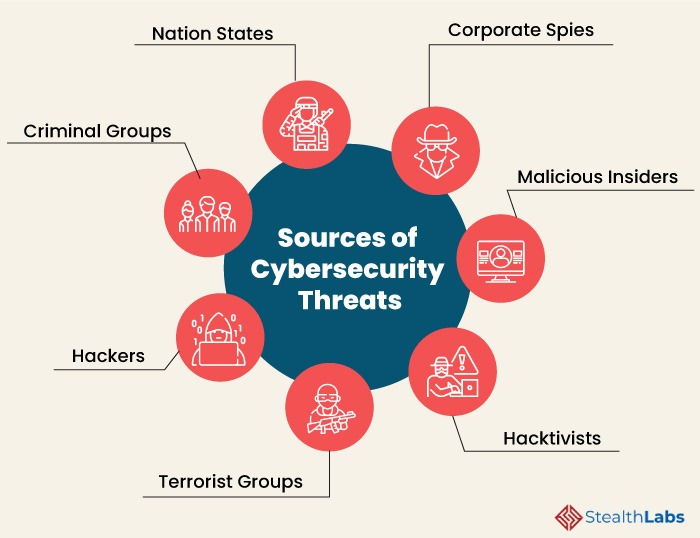
1. **Cross-site scripting**

Cross-site scripting (XSS) is a code injection security attack targeting web applications that delivers malicious, client-side scripts to a user’s web browser for execution.

**Sources of Cybersecurity Threats**

Cyber threats come from a variety of places, people and contexts. Malicious actors include:

* Individuals that create attack vectors using their own software tools
* Criminal organizations that are run like corporations, with large numbers of employees developing attack vectors and executing attacks
* Nation states
* Terrorists
* Industrial spies
* Organized crime groups
* Unhappy insiders
* Hackers
* Business competitor



**Cyber security Best Practices to Protect from Cyber Threats**

**–**

**Conclusion**

Today due to high internet penetration, cyber security is one of the biggest need of the world as cyber security threats are very dangerous to the country’s security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free.

**References**

1. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
2. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
3. https://www.cisco.com/c/en\_in/products/security/common-cyberattacks.html
4. IEEE Security and Privacy Magazine – IEEECS “Safety Critical Systems – Next Generation “July/ Aug 2013