# Types of Cyber Threats- Malware, phishing, ransomware, DDoS attacks, and insider threats

---

**1. Malware**

**Definition**: Malware, short for "malicious software," refers to any software intentionally designed to harm or exploit devices, networks, or services.

**Common Types**:

- **Viruses**: Attach themselves to legitimate programs and spread when executed.
- **Worms**: Self-replicating programs that spread across networks without user interaction.
- **Trojans**: Disguised as legitimate software but perform malicious activities when executed.
- **Spyware**: Collects sensitive information without the user's consent.
- **Adware**: Delivers unwanted advertisements, often leading to additional malware.

**Impact**: Data theft, system damage, unauthorized access, and financial loss.

---

**2. Phishing**

**Definition**: Phishing is a social engineering attack where attackers deceive individuals into providing sensitive information, such as login credentials, financial details, or personal data.

**Methods**:

- **Email Phishing**: Fraudulent emails designed to appear from trusted entities.
- **Spear Phishing**: Targeted phishing attacks aimed at specific individuals or organizations.
- **Smishing and Vishing**: Phishing attempts via SMS (smishing) or voice calls (vishing).

**Impact**: Identity theft, financial fraud, and unauthorized access to systems or accounts.

---

**3. Ransomware**

**Definition**: Ransomware is a type of malware that encrypts a victim's data and demands payment (usually in cryptocurrency) to restore access.

**Characteristics**:

- **Encrypting Ransomware**: Locks files and requires a decryption key for access.
- **Locker Ransomware**: Prevents access to the entire system.

**Famous Examples**: WannaCry, Petya, and REvil.

**Impact**: Operational disruptions, financial loss, and data breaches.

---

**4. Distributed Denial-of-Service (DDoS) Attacks**

**Definition**: A DDoS attack overwhelms a target system, network, or service with excessive traffic, rendering it unavailable to legitimate users.

**Mechanism**:

- Attackers use a network of compromised devices (botnets) to flood the target with requests.

**Impact**:

- Service outages, loss of revenue, reputational damage, and potential security vulnerabilities.

---

### 5. Insider Threats

**Definition**: Insider threats originate from individuals within the organization who intentionally or unintentionally compromise security.

**Types**:

- **Malicious Insiders**: Employees or contractors with harmful intent, such as stealing data or sabotaging systems.
- **Negligent Insiders**: Users who unintentionally cause security incidents through errors or carelessness (e.g., clicking on phishing links).

**Impact**: Data theft, reputational damage, financial losses, and compromised intellectual property.

---

### Conclusion

Understanding these types of cyber threats is crucial for implementing effective security measures. Each threat type requires tailored strategies, including employee training, robust security technologies, and regular monitoring, to mitigate risks and protect organizational assets.