**Types of Security Threats**

**Phishing** is using forged messages to achieve personal information. It is done with using a fake e-mail address and website. Phishing uses the victim’s trust to lure them into clicking a dangerous link that would enable the criminal to achieve sensitive information which can then be used either by the criminal or sold to third parties for cash.

[**Spoofing**](https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/)is a technique through which a cybercriminal disguises themselves as a known or trusted source to engage with the target and access their systems or devices with the ultimate goal of stealing information, extorting money or installing malware or other harmful software on the device.

## **Code Injection Attacks** consist of an attacker injecting malicious code into a vulnerable computer or network to change its course of action.(SQL injection or cross site scripting)

**I**[**nsider threats**](https://www.crowdstrike.com/cybersecurity-101/insider-threats/)are internal actors such as current or former employees that pose danger to an organization because they have direct access to the company network, sensitive data, and intellectual property (IP), as well as knowledge of business processes, company policies or other information that would help carry out such an attack.

## **DNS Tunneling** is a type of cyberattack that leverages domain name system (DNS) queries and responses to bypass traditional security measures and transmit data and code within the network.

**Malware** is an abbreviation of “malicious software”, which includes viruses, worms, trojans, spyware, and ransomware, and is the most common type of cyberattack.

**Ransomware** is a type of malware that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid.

**A** [**Denial-of-Service (DoS)** attack](https://www.crowdstrike.com/cybersecurity-101/denial-of-service-dos-attacks/) is a malicious, targeted attack that floods a network with false requests in order to disrupt business operations.

They cost the organization time, money and other resources in order to restore critical business operations.

DDoS attacks are launched from multiple systems.