# Task 1: Learn Network Security Concepts

**Network Threats:**

**Virus:**

A malicious program that attaches to files and replicates itself to spread. Often damages or corrupts files.

**Worm:**

Self-replicating software that spreads across networks without user intervention, often consuming bandwidth or overloading systems.

**Trojan:**

A type of malware disguised as legitimate software that enables unauthorized access or control once installed.

**Phishing:**

A social engineering attack that tricks users into revealing personal or sensitive information via deceptive emails or websites.

**Basic Security Concepts:**

**Firewall:**

A hardware or software security system that monitors and controls incoming and outgoing network traffic based on predetermined rules. Protects against unauthorized access.

**Encryption:**

The process of converting data into a coded format to prevent unauthorized access. Ensures confidentiality during data transmission or storage.

**Secure Network Configuration:**

Involves best practices like changing default passwords, disabling unused ports, and using WPA2/WPA3 for Wi-Fi security to reduce vulnerabilities.