# Topic: Cyber Security Threats

It's important to understand that cyber security threats are actions taken by hackers or cybercriminals to compromise a computer system or network. These threats can result in unauthorized access to data, system damage, or even financial loss. Here are some of the most common cyber security threats and their processes:

**Brute-force attack:** This is a type of attack where a hacker tries to gain access to a system or account by guessing the password through trial and error. They use software that automatically tries different combinations of passwords until the right one is found.

**Data interception:** This is the act of intercepting data as it's transmitted across a network. Hackers use specialized tools to intercept data packets and extract sensitive information such as passwords or credit card numbers.

**Distributed Denial of Service (DDoS) attack:** In this type of attack, hackers flood a website or network with traffic to overwhelm the server and make it unavailable to legitimate users. Hackers often use a botnet, which is a network of compromised computers, to carry out a DDoS attack.

**Hacking:** Hacking refers to the act of gaining unauthorized access to a computer system or network. Hackers use a variety of techniques such as exploiting vulnerabilities in software or social engineering to gain access to sensitive information.

**Malware:** Malware refers to any type of software designed to harm a computer system or network. It includes viruses, worms, Trojan horses, spyware, adware, and ransomware. Hackers use different types of malware to steal data, gain access to a system, or cause damage.

**Pharming:** This is a type of cyber attack where a hacker redirects a website's traffic to a fake website that looks like the original. The purpose is to steal sensitive information such as passwords or credit card numbers.

**Phishing:** Phishing is a type of social engineering attack where a hacker sends an email or message that appears to be from a legitimate source, such as a bank or social media platform. The message usually contains a link or attachment that, when clicked, installs malware or takes the user to a fake website where they are prompted to enter sensitive information.

**Social engineering:** Social engineering refers to the act of manipulating people to divulge sensitive information or perform an action that benefits the hacker. It can take many forms, such as phishing.

## Topic: Cyber Security Threats

The aim of these cyber security threats is usually to gain unauthorized access to a computer system or network, steal sensitive information, cause damage, or disrupt operations. It's important to take measures to protect your devices and data by using strong passwords, keeping software up-to-date, and being vigilant for suspicious activity.