Understanding Denial-of-Service Attacks

What is a denial-of-service (DoS) attack?

In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. When you type a URL for a particular website into your browser, you are sending a request to that site's computer server to view the page. The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process your request. This is a "denial of service" because you can't access that site.

An attacker can use spam email messages to launch a similar attack on your email account. Whether you have an email account supplied by your employer or one available through a free service such as Yahoo or Hotmail, you are assigned a specific quota, which limits the amount of data you can have in your account at any given time. By sending many, or large, email messages to the account, an attacker can consume your quota, preventing you from receiving legitimate messages.

What is a distributed denial-of-service (DDoS) attack?

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer. He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

How do you avoid being part of the problem?

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- Install and maintain anti-virus software.
- Install a firewall, and configure it to restrict traffic coming into and leaving your computer.
- Follow good security practices for distributing your email address .
- Applying email filters may help you manage unwanted traffic.

How do you know if an attack is happening?

Not all disruptions to service are the result of a denial-of-service attack. There may be technical problems with a particular network, or system administrators may be performing maintenance. However, the following symptoms could indicate a DoS or DDoS attack:

- unusually slow network performance (opening files or accessing websites)
- unavailability of a particular website
- inability to access any website
- dramatic increase in the amount of spam you receive in your account

What do you do if you think you are experiencing an attack?

Even if you do correctly identify a DoS or DDoS attack, it is unlikely that you will be able to determine the actual target or source of the attack. Contact the appropriate technical professionals for assistance.

If you notice that you cannot access your own files or reach any external websites from your work computer, contact your network administrators. This may indicate that your computer or your organization's network is being attacked.

If you are having a similar experience on your home computer, consider contacting your internet service provider (ISP). If there is a problem, the ISP might be able to advise you of an appropriate course of action.