In DOS attack (Denial of Service attack), a single attacker attacks a single target i.e. one computer and one internet connection is used to flood the server with packets. Attacker sends a large number of legitimate looking requests to the server in a way that the server cannot really distinguish between valid and invalid requests. It will overwhelm the system to a point that the server cannot handle the capacity anymore. The aim is to overload the targeted server bandwidth and other computing resources. This will make the server inaccessible to other.

In DDOS attack (Distributed Denial of Service attack), the attacker develops a specialized malware which spreads to as many vulnerable computers as possible which are distributed around the whole world via compromised websites, emails or even organization’s network. The tricked users turn their computers into a bot and provide access points to command and control server. Thousands of bots form a botnet. The botnet owners send message to command and control server with instruction to attack particular target. Then botnet follow the orders from command and control server and attack the target.

Prevention methods:

1. Not opening any unknown links.

2. Get professional company to mitigate it which will install Net Flow protocol that monitors traffic to your website.

3. If you are serving your own data, make sure all your routers drop junk packets, block ICMP when you don’t need it and setup strong firewall.