DoS

1. Denial of Service (DoS) attacks: A DoS attack is an attempt to make a website or network unavailable to users by overwhelming it with traffic from multiple sources.
   1. TCP SYN Flood: This attack exploits the way that a TCP connection is established, by flooding a server with a high volume of SYN packets, which results in the server becoming unresponsive or crashing.
   2. UDP Flood: This attack involves flooding a server with a high volume of UDP packets, which can consume network resources and cause the server to become unavailable.
   3. Ping of Death: This attack involves sending an oversized ping packet to a server or network device, which causes the device to crash or become unresponsive.
   4. Smurf Attack: This attack involves sending a high volume of ICMP echo requests to a network's broadcast address, causing all devices on the network to respond and overload the network.
   5. Application Layer DoS: This attack targets the application layer of a network, by overwhelming the server with requests that are designed to consume resources or crash the application.
   6. Distributed DoS (DDoS): A DDoS attack involves using multiple compromised devices (often through botnets) to simultaneously target a single server or network, overwhelming it with traffic and making it unavailable, which is probably the most common one.
2. Cyber-attacks affecting casual internet user:
   1. Just as they can overwhelm and crash a website, they can also do that to a home router and stop access to the internet for the whole household.