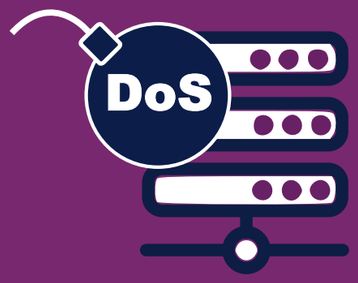
National Cyber Security Centre

Denial of service (DoS)
Preparing for DoS attacks

This advice is written for **technical and security IT professionals**, and summarises how to prepare for denial of service (DoS) attacks. It is not possible to fully mitigate the risk of a DoS attack affecting your service. However, the following five practical steps, if implemented, will lessen the impact of any incident.

About DoS and DDoS attacks



A **denial of service** (DoS) attack occurs when users are denied access to computer services (or resources), usually by overloading the service with requests.

An attack becomes a '**distributed denial of service**' (DDoS), when it comes from multiple devices. This is the most common form of DoS attack on **websites**. However, attacks on any type of **system** - including industrial control systems which support critical processes - can result in a denial of service.

DoS attacks are one of the modern cyber criminal's favourite tools; they're effective against some of the strongest targets, yet comparatively cheap and easy to run. The only reliable way to weather a DoS attack is to **be prepared**, to remain vigilant and to act swiftly when an attack begins.

© Crown Copyright 2019

1. Understand your service



Understand how your service can be overloaded or exhausted. Find out whether you (or a supplier) are responsible for:

- **Network connectivity**: the network links between your service and your users (or between components in your service) could be saturated by illegitimate traffic.
- **Compute**: the amount of computing resource available to service legitimate requests can be overwhelmed by a surge in malicious sessions.
- **Storage**: an attacker may attempt to consume your available storage capacity.

2. Upstream defences

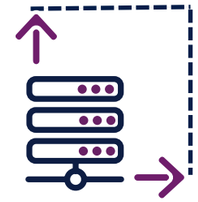


Ensure your service providers are ready to deal with resource exhaustion in places where they are uniquely placed to help.

We recommend you:

- Understand the **DoS mitigations** that your ISP can enable on your account.
- Consider deploying a **Content Delivery Network**, for web-based services.
- Understand when your service providers would **throttle access** to protect their other customers.
- Consider using **multiple service providers** for some functionality.

3. Build to allow scaling



To deal with attacks which can't be handled upstream (or only once detected and blocked), make sure your service can **rapidly scale**.

Ideally, you can scale all aspects of your application and infrastructure. Cloud-native applications can be automatically scaled using the cloud providers' APIs.

In private data centres, automated scaling is possible using modern virtualisation, but this will require spare hardware capacity to deal with the additional load.

4. Define your response plan



Design your service so that when attacked, it can **continue to operate**, albeit in a degraded fashion.

We recommend your plan includes:

- graceful degradation
- dealing with changing tactics
- retaining administrative access during an attack
- having a scalable fall-back plan for essential services

5. Test and monitor your services



Gain confidence in your defences by testing them, and ensure you can spot when attacks start by having the **right tools in place**.

Thinking you are well prepared for DoS attacks is not the same as knowing. Test your defences so you know the types (and volume) of attacks you are able to defend.

System monitoring will help you spot attacks when they begin, and analyse your response while it's underway.