What to do when your website goes down

A threat that many independent journalists, news sites, and bloggers face is having their voices muted because their website is down. In many cases, this may be an innocent if frustrating problem, but on occasion, it may be due to a “denial of service” attack.

This document will walk you through some very basic steps to diagnose potential problems. If your site is under a denial of service attack, some immediate options for next steps are suggested. Even if you have not experienced a denial of service attack, this guide offers steps to prepare for one -- hopefully preventing any downtime at all.

- What to do when your website goes down
- First Steps: Diagnosing other potential problems
- Next Steps
- Responding to a Denial of Service Attack
  - Hosted Services
  - Proxied Services
  - Mixed and Custom Options
  - Before you choose
    - For all services:
    - For hosted services
    - For proxied services:
- Mitigation Services
  - Hosted Services
    - VirtualRoad.org
    - More Secure Hosting Organizations:
  - Proxy Services
    - Deflect
    - CloudFlare
    - Google’s PageSpeed
  - Related Services: Domain Name Registration
- Glossary

First Steps: Diagnosing other potential problems

Sites most often go down due to programming errors or technical problems at the company that hosts the site. Sometimes, other things like legal challenges can cause a host to turn a site off as well. Let’s first try to check for these common problems. When possible, the best first step is to contact a trusted person who can help with your website (your webmaster, the people who helped you set up your site, your internal staff if you have them, and the company that hosts your site).

If you are currently researching how to build your website to be resistant to attacks that might take it offline, you should first read through this guide by the Electronic Frontier Foundation: https://www.eff.org/keeping-your-site-alive .

AccessNow provides a much more in-depth guide with many more resources and mitigation techniques in English, Farsi, Arabic, and Russian. Visit https://www.accessnow.org/policy/docs and click on DoS on the right side, or download a copy from https://s3.amazonaws.com/access.3cdn.net/3fd9faf32feb878cf7_krm6iy7bo.pdf .

1. Are you seeing error messages? This is a **software problem**, and you should contact your webmaster. Sending your webmaster a screenshot, the link of the page you are having problems with, and any error messages you see will help them figure out what might be the cause of the problem. You might also copy the error messages into a search to see if they are easily fixed.
2. Your hosting company may be having problems, in which case you may be facing a **hosting problem**. Can you visit the website of your hosting company? Note that this is ***not*** the admin section of your own site, but the company or organization you work with to host your site. Look or search for a "status" blog (e.g. status.dreamhost.com), and also search on twitter.com for other users discussing downtime at the host - a simple search like "(company name) down" can often reveal if many others are having the same problem.
3. If your site is loading extremely slowly or not at all, check http://www.isup.me/ - your site might be up, but you can't see it. This is a **network problem**. Your own Internet connection could be having problems or be blocking your access to your site. Try visiting other pages on the Internet. Can you visit other sites with content like your site? Try using Tor (https://www.torproject.org/projects/gettor.html) or Psiphon (https://psiphon.ca/products.php) to access your site. If this helps, you have a **blocking problem**, but you are still online for other parts of the world.
4. ***Contact your webmaster and the site host!*** The problem you face may not be reported on their status page yet, or you could have been taken offline for other reasons (a legal/copyright request, for example). This is a **legal problem**, and the resources provided by the EFF, while focused on US copyright laws, are a good place to learn more: https://www.eff.org/issues/bloggers/legal/liability/IP.

In addition to the services and suggestions below, it's always good to make sure you have backups (that you store somewhere other than the same place your website is!) - many hosts and website platforms have this included; but it's best to also have additional copies. Also ensure that your website technology is updated to the latest software.

Next Steps

If there is not a legal or technical problem above, your site may be overwhelmed by the number and speed

of requests for pages it is receiving -- this is a **performance problem**. This could be "good" in that your site has become more popular and it simply needs some improvements to respond to more readers - check your site analytics for a long-term pattern in growth. Contact your webmaster or hosting provider for guidance. Many popular blogging and CMS platforms (Joomla, Wordpress, Drupal...) have plugins to help cache your website locally and integrate CDNs, which can dramatically improve site performance and resilience. Many of the solutions below can also help performance problems as well.

Your site may be the victim of a **"denial of service" attack**, where a malicious user (or many of them), try to view the website over and over again, quickly (using automated tools), and in doing so crowd out legitimate readers. Sometimes it's one "attacker" trying to do this to your site, which usually doesn't cause much of a problem -- unless you pay for bandwidth. More common is the "Distributed" denial of service (DDoS), where an attacker who controls thousands of machines targets a site with all of them.

Imagine hundreds of people in line at a food stall who, when they get to the front of the line, slowly decide not to order anything, but then immediately get back in line. There may be legitimate customers in line, but it's going to take them hours to get their food, and the vendor may give up!

Responding to a Denial of Service Attack

Don't wait until you have been attacked! All of the services listed below will work quickly to help you recover during or after an attack, but you can get protected now, before any attack happens! This can reduce costs by lowering your bandwidth usage, and keep you online during an attack. Once you've been hit, it can take up to three days for the Internet to "find" you at your new, protected address - so in almost every case, it's much better to **be prepared and get started now**. The first step is to work with the company you bought your domain from, and change the "Time to Live" or TTL to 1 hour. This can help you redirect your site once it comes under attack much faster (the default is 72 hours, or three days).

There are many services that can help you with denial of service attacks; and they fall (very broadly) into two categories - **hosted** and **proxy** services.

Hosted Services

Hosted services require you to move your website completely to their servers - you're changing hosting providers. Many of them can help you through this. The benefits of this include the hosted solution often providing many other protection features in addition to DDoS mitigation; the downside can be cost (depending on what you currently pay) and control - you need to be able to trust your domain host, as they have a lot of control over your website. Hosted services may also use a mixture of the same technology as proxy services below.

Pros:

- Provides one central service for most, if not all, your website needs
- Often includes many secondary services and consulting, and even limited legal defense in some cases

- Full support teams often on staff to help

Cons:

- You must host your website with the service
- You must trust the service to manage your site and defend your rights
- These services often are much more expensive (but you don't have to pay other hosting / DNS services anymore!)

Proxied Services

Proxied services let you continue hosting your site wherever it is, and just change how others on the Internet find and access it - this is generally much easier to set up. These services have servers around the world which essentially get out in front of your website and absorb or ignore malicious traffic. They serve constantly-updated copies of your site. These services are very easy to set up, and you maintain complete control of your website and hosting setup. One challenge with proxied services is that very complex websites can sometimes experience problems with non-admin user logins and complex interactive/javascript area. Please discuss these with your webmaster and the proxy service as most can be resolved.

Pros:

- Lower cost (often with a free level)
- Quick and easy to set up
- You don't have to change your existing website host
- You can change or quit the service at any time

Cons:

- Fewer support options
- Focused primarily on just mitigating DDoS attacks - does not necessarily include help with malware, spammers, etc.
- SSL (encrypted) traffic will be briefly decrypted and re-encrypted by the proxy server to pass it from their proxy to your server.

Custom Options

It's important to note that there are many ways to combine these approaches. Many websites use what is called a Content Delivery Network (CDN), which takes some of the burden (serving images and other static content) off of a website and speeds it up greatly. Dynamic sites (such as those powered by content management systems like Joomla, Wordpress and Drupal), can sometimes be "converted" into static sites that can be fully hosted (mirrored) using CDNs.

Content Delivery Networks can help reduce bandwidth costs and load during DDoS attacks, which, if your host is powerful enough for the rest, can get you through. There are hundreds of CDN services, including Akamai and Amazon CloudFront. MaxCDN has a free level of service, but generally, cost scales with bandwidth, meaning that these may become a financial drain during a DDoS attack. These often require a bit of technical expertise to get working, and you should work with your webmaster.

Before you choose

Finally, for any service, you must be comfortable with the provider - that means trust, but also understanding their business model: Is it fee-for-service? If there's a free version, does it receive less support than a paid alternative? Is it funded by governments? It is best to cover as much detail up front as possible to avoid surprises down the road.

For all services:

- How is the company/organization structured and sustained? What types of vetting or reporting are the required to do, if any?
- Consider what country/countries they have a legal presence in and would be required to comply with law enforcement and other legal requests
- What logs are created, and for how long are they available?
- Are there restrictions that impact you on what content the service will host/proxy?
- Are there restrictions on the countries where they can provide service?
- Do they accept a form of payment you can use?
- Secure communications -- you should be able to log in securely, communicate with the service provider securely, and ideally have a "two factor" authorization for major changes
- What type of ongoing support will you have access to? Is there an additional cost for support, and/or will you receive sufficient support if you are using a "free" tier?
- Can you "test-drive" your website before you move over via a staging site?

For hosted services

- Do they offer full support on moving your site over?
- Are the services equal or better options than your current host, at least for tools/services you use? Top things to check are:
    - Management dashboards like cPanel
    - Email accounts (how many, quotas, access via SMTP, IMAP)
    - Databases (how many, types, access)
    - Remote access via SFTP/SSH
    - Support for the programming language (PHP, Perl, Ruby, cgi-bin access...) or CMS (Drupal, Joomla, Wordpress…) your site uses
- Is there an option for two-factor authentication, to improve the security of administrator access? This or related secure access policies can help reduce the threat of other forms of attacks against your website.

For proxied services:

- If you use SSL, ask how they manage SSL. In some configurations, it may be easiest to share your private SSL key. If you do so, you need to have a high level of trust in the service provider, as they can "impersonate" your site (indeed, this is what you are asking them to do by providing a

proxy!)
- Ask about how administration / editorial logins and pages are managed
- Talk about any interactive parts of your website (users who log in, comment, admin/editorial needs, complex interactive pages/javascript/animations) -- different proxy services manage these differently; you will need to test these before switching completely.

Mitigation Services

All of the services listed below provide protection against DDoS attacks. This is not a complete listing of services - there are many, many more. These services all represent good starting points, as they have been used by other members in the independent media / human rights / free speech communities.

Hosted Services

This by no means is an exhaustive list. It focuses on services which can be initiated quickly and have strong track-records on protecting free speech online. Please note that prices for hosted services are not directly comparable to those of proxy services. Hosted services will take the place of any existing cost for website hosting.

VirtualRoad.org

- **Cost:** Pricing starts at €100/month for simple sites. Other tiers for more complex hosting needs or higher resource demands are available.
- **Restrictions:** None, though the service is focused on content management systems which use PHP (Joomla, Drupal, Wordpress, and similar)
- **About the organization and its business model:** VirtualRoad.org is part of Media Frontiers, a social purpose enterprise registered in Denmark as an ApS / limited liability company, established by the press freedom NGO, International Media Support (IMS). IMS is funded largely by the governments of Denmark, Sweden, and Norway. This organizational structure is meant to build long-term sustainable services for the community.
- **Additional Services:** VirtualRoad.org offers full-range protection encompassing a wide variety of services, from transferring your site to their systems, domain registration, optimization, security audits, protection from hacking and phishing, security reports detailing attempted attacks, and even support in responding to legal requests. See https://virtualroad.org/get-protected/packages for more details.
- **Technical needs:** You will need to have full access to your website's backend or backups, as well as to edit your nameservers. If you need technical assistance with any of the onboarding or hosting, VirtualRoad.org will support you through the process.
- **Get Started Now:** Visit https://virtualroad.org/contact or email info@virtualroad.org

The Positive Internet Company

- **Cost:** Pricing starts at $495/month for fully managed servers. Shared hosting may be available for only £125/year.

- **Restrictions:** None
- **About the organization and its business model:** The Positive Internet Company is a for-profit company with offices in the UK and the US.
- **Additional Services:** Services are fully managed, including firewalls, databases, and backups. More information available here: http://www.positive-internet.com/services/vip-hosting
- **Technical needs:** You will need to have full access to your website's backend or backups, as well as to edit your nameservers. The Positive Internet Company provides technical assistance with onboarding and hosting.
- **Get Started Now:** Visit http://www.positive-internet.com/contact-us or email good@positive-internet.com

More Secure Hosting Organizations:

- **Greenhost**: https://greenhost.nl/order/ Greenhost is a Dutch company founded to provide sustainable, environmentally friendly website hosting services. Greenhost is committed to an open and free internet, and the protection of its users.
- **Ecological and Dissident Hosting**: https://ecodissident.net/hosting EcoDissident focuses on providing strong protection for free speech; you may want to pair hosting here with a proxied service, below)
- **Gandi.net** https://www.gandi.net/ . Gandi is based in Paris (France), with offices in Baltimore (USA) and Vancouver (Canada), and supports many popular community tools and projects.
- **Many others!** There are many other organizations who are aligned with promoting Internet freedom and can help you recover from a DDoS in various ways.

Proxy Services

Again, this is by no means an exhaustive list; there are thousands of commercial services which offer variants of proxy and CDN tools which can help defend against DDoS attacks. This list focuses on services which can be initiated quickly and have strong track-records on protecting free speech online.

Deflect

- **Cost:** Free
- **Restrictions:** NGOs, human rights, independent media
- **About the organization and its business model:** Deflect is an open source project of eQualit.ie, a not-for-profit technology collective based in Montreal, Canada with deep roots in the human rights technology community. Deflect is funded by NGOs and governments, including the US government, to provide Deflect services to protect the freedom of speech. Deflect does not disclose the websites they protect nor need approval to provide service. Deflect maintains servers with like-minded hosting companies around the world.
- **Additional Services:** The Deflect team will support you getting on to their services. They have some grant funding available to pay for additional SSL Certificates and other related protection/recovery costs. Sites protected by Deflect can opt to add additional layers of security to their core site.

- **Technical needs:** You will need the ability to change your nameservers.
- **Get Started Now:** https://wiki.deflect.ca/signup/. See also https://wiki.deflect.ca/wiki/Join_Deflect

CloudFlare

- **Cost:** Free for basic protection, $20/month to include SSL support, and up to $200/month for more advanced needs. Paid customers receive preferential support and uptime guarantees.
- **Restrictions:** Subject to US export controls, see also https://blog.cloudflare.com/thoughts-on-abuse
- **About the organization and its business model:** Cloudflare is a privately-held Delware-incorporated US for-profit company based in San Francisco. They maintain servers around the world (https://www.cloudflare.com/network-map) and comply with legal requests.
  It should be noted that part of CloudFlare's defenses against DDoS attacks occasionally degrade access from the Tor network. This happens if someone is using Tor to abuse a service, and is *not* a policy decision to block Tor.
  Cloudflare is required to comply with US legal requests and National Security Letters.
- **Technical needs:** You will need the ability to change your nameservers.
- **Get Started Now:** Create an account here: https://www.cloudflare.com/sign-up

Google's PageSpeed

- **Cost:** Free during trial period. There will be a 30-day notice before it changes to a fee-based model.
- **Restrictions:** You must be approved, generally a 2-hour process, but may be restricted for some organizations or countries.
- **About the organization and its business model:** Google is an international, public, for-profit company based in Mountain View, California, USA.
  As with most Google products, this ties the Google account you use to your website. This service falls under Google's overall privacy policy and terms of service.
  Google is required to comply with US legal requests and National Security Letters.
- **Technical needs:** You will need the ability to fine-tune your DNS records. PageSpeed rewrites and optimizes some parts of your website, which can alter functionality; you should be ready to test for this.
- **Get Started Now:** Begin the sign-up process here: https://developers.google.com/speed/pagespeed/service

Related Services: Domain Name Registration

DDoS attacks also impact many other services around your website - the service that directs visitors to the right webserver (DNS servers or name servers) may also be attacked or impacted. While the services you engage below will support you in chosing/moving DNS providers, here is a short list of well-regarded services. EasyDNS and Hover.com are based in Canada, 1984.is, Iceland.

- EasyDNS https://web.easydns.com/
- 1984.is https://www.1984.is/

- Hover.com https://www.hover.com/

Glossary

- **CDN / Content Delivery Network**: A worldwide collection of computers you can program your website to use to serve content quickly. Consider the case where your website is hosted in Iceland, but you have visitors from Thailand. If you use a CDN, at least parts of your site can be delivered to the visitor from a computer that is much closer to them, than having to come all the way from Iceland. This also has the effect of spreading the load out among other computers, which can reduce the severity of a DDoS Attack
- **DDoS / Distributed Denial of Service Attack**: a "denial of service" attack is where a malicious user (or many of them), try to view the website over and over again, quickly (using automated tools), and in doing so crowd out legitimate readers. Sometimes it's one "attacker" trying to do this to your site, which usually doesn't cause much of a problem -- unless you pay for bandwidth. More common is the "Distributed" denial of service (DDoS), where an attacker who controls thousands of machines targets a site with all of them.
- **Domain Name:** The human-readable name of your website - google.com, for example.
- **DNS Record**: The DNS record is like the master Contact List of Phone Book of the Internet. All website servers are identified by a series of numbers and/or coded letters (the IP Address) - Google.com is 74.125.228.69, for example. By changing this record, you can give out a different IP Address for a website - which could be a new hosting provider's address or a proxy for your original website.
- **Nameserver:** When a browser wants to find a website, it will first contact a name server, which will tell connect the domain name (google.com) to it's Internet address / IP Address (74.125.228.69) via it's DNS Record (above). By changing the DNS record at a name server, you can "point" the browser to a different server.
- **Website host**: The server where your website and its files/databases are stored.