


We all want to keep our kids safe from the nastiness that lurks out on the Internet. This article will show how to use [Open DNS](#) with any Operating System (MAC Windows Linux etc.) to help filter undesirable web content. Simply put [DNS \(Domain Name System\)](#) translates IP address to an easy to remember hostname. For example if you were to type "216.239.51.99" without the quotes into your web browser you will be directed to google.com.

Previously I have written an article that introduces you to Open DNS and how to add it to your router. I have attached that article to the end of this one for those of you that missed it. Here we will look a bit deeper into it and show you how to best use OpenDNS to your advantage. There are a lot of web content filtering possibilities which include specific sites, specific content, and adult website filtering.



The first thing you will want to do is sign up for a free account and download the OpenDNS Updater application. OpenDNS will automatically detect your IP address and will prompt you to create a name and download the Updater application.

You've successfully added a network! Just a few more steps and you're home free.







1. Give it a friendly name:
Something simple like "Office" or "Home" will do.
2. Is this a dynamic IP address? [What is a dynamic IP address?](#)
 Yes, it is dynamic
3. Download the software and stay safe. The OpenDNS Updater software ensures that your OpenDNS preferences are preserved whenever your IP address changes.
 [OpenDNS Updater for Windows](#)

[» Updater for other platforms](#) DONE



After signing up go to your Dashboard where you can start creating rules for filtering, manage your administrator settings, and add additional networks. Basically your dashboard is where you will make all changes you need. If you ever get stuck or have questions they also have a cool support system which includes a knowledge base and user forum.

Manage your account


You haven't added a **logo** yet. [Add one now...](#)
You haven't created any **shortcuts** yet. [Create one now...](#)

 <h3><u>Stats</u></h3> <p>Get insight into your network activity.</p>	 <h3><u>Settings</u></h3> <p>Manage how OpenDNS works on your networks.</p>
 <h3><u>Networks</u></h3> <p>Add or remove networks from your account.</p>	 <h3><u>Shortcuts</u></h3> <p>Set up network shortcuts.</p>
 <h3><u>Support</u></h3> <p>Need help?</p>	 <h3><u>My Info</u></h3> <p>Edit your personal information.</p>

Spread the word

 <h3><u>Tell A Friend</u></h3> <p>Tell your friends and colleagues about OpenDNS.</p>	 <h3><u>OpenDNS Buttons</u></h3> <p>Put an OpenDNS button on your site.</p>
--	--

Communicate with your users

 <h3><u>OpenDNS Intro</u></h3> <p>Share this link to introduce the benefits of OpenDNS.</p>
--

Lets take a look at filtering content. From your dashboard click on Settings. You will then be prompted to choose a basic filtering level from None to High. This might be a good choice if you want to easily filter out several categories. To view what the categories are in each level just click on View for a detailed look.

Choose your filtering level

- High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. [27 categories in this group - View](#) - [Customize](#)
- Moderate** Protects against all adult-related sites and illegal activity. [14 categories in this group - View](#) - [Customize](#)
- Low** Protects against pornography and phishing. [5 categories in this group - View](#) - [Customize](#)
- Minimal** Protects against phishing attacks. [1 category in this group - View](#) - [Customize](#)
- None** Nothing blocked.
- Custom** Choose the categories you want to block.

APPLY









This is an example of the detailed categories in the Low filter setting. This helps you choose what types of content you want blocked.

Sexuality
Sites that provide information, images or implications of bondage, sadism, masochism, fetish, beating, body piercing or self-mutilation.

Pornography
Anything relating to pornography, including mild depiction, soft pornography or hard-core pornography.

Phishing Protection
By enabling phishing protection, you'll protect everyone on your network from known phishing sites using the best data available.

Here is a list of all the categories available to block through OpenDNS. As you can see this service will work for your children as well as any user on your network and also for business.

<input type="checkbox"/> Adult Themes 	<input type="checkbox"/> Adware	<input type="checkbox"/> Alcohol
<input type="checkbox"/> Auctions	<input type="checkbox"/> Automotive	<input type="checkbox"/> Blogs
<input type="checkbox"/> Business Services	<input type="checkbox"/> Chat	<input type="checkbox"/> Classifieds
<input type="checkbox"/> Dating	<input type="checkbox"/> Drugs	<input type="checkbox"/> Ecommerce/Shopping
<input type="checkbox"/> Educational Institutions	<input type="checkbox"/> File storage	<input type="checkbox"/> Financial institutions
<input type="checkbox"/> Forums/Message boards	<input type="checkbox"/> Gambling	<input type="checkbox"/> Games
<input type="checkbox"/> Government	<input type="checkbox"/> Hate/Discrimination	<input type="checkbox"/> Health
<input type="checkbox"/> Humor	<input type="checkbox"/> Instant messaging	<input type="checkbox"/> Jobs/Employment
<input type="checkbox"/> Lingerie/Bikini 	<input type="checkbox"/> Movies	<input type="checkbox"/> Music
<input type="checkbox"/> News/Media	<input type="checkbox"/> Non-profits	<input type="checkbox"/> Nudity 
<input type="checkbox"/> P2P/File sharing	<input type="checkbox"/> Parked Domains	<input checked="" type="checkbox"/> Phishing 
<input type="checkbox"/> Photo sharing	<input type="checkbox"/> Podcasts	<input type="checkbox"/> Politics
<input type="checkbox"/> Pornography 	<input type="checkbox"/> Portals	<input type="checkbox"/> Proxy/Anonymizer 
<input type="checkbox"/> Radio	<input type="checkbox"/> Religious	<input type="checkbox"/> Research/Reference
<input type="checkbox"/> Search engines	<input type="checkbox"/> Sexuality 	<input type="checkbox"/> Social networking
<input type="checkbox"/> Software/Technology	<input type="checkbox"/> Sports	<input type="checkbox"/> Tasteless 
<input type="checkbox"/> Television	<input type="checkbox"/> Travel	<input type="checkbox"/> Video sharing
<input type="checkbox"/> Visual search engines	<input type="checkbox"/> Weapons	<input type="checkbox"/> Webmail

You can choose a filtering level and add customized domain filtering to it, or completely customize everything. Probably one of the more publicized social sites you may want to block your child from is MySpace so I will use it as my example. Below the filtering levels you will see *Manage individual domains*. This is where you can get more specific in what your filtering. The two options are Never Block or Always Block.

Manage individual domains

If there are domains you want to make sure are always blocked (or always allowed) regardless of the categories blocked above, you can add them below.

Hint: to block *all* subdomains, block myspace.com.
I want to block: myspace.com or www.myspace.com

Always block ▾

ADD DOMAIN

Just type in the address of the site to block and click on the Add Domain button. You can then choose to just block the domain or better yet, block all of the categories in the sub-domain. This means although you block myspace.com if you do not block the sub-domains within the user can access some of the content. Any changes you make will take about 3 minutes to update.

You can block www.myspace.com two different ways.

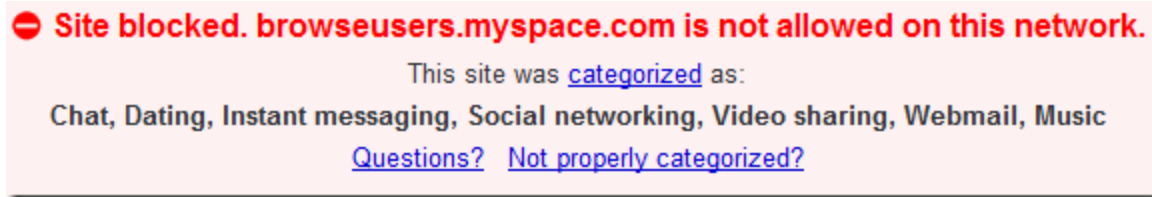
Block www.myspace.com — just the individual domain.

I'd rather block categories of websites that include www.myspace.com

- Chat
- Dating
- Instant messaging
- Social networking
- Video sharing
- Webmail
- Music

CONFIRM or [cancel](#)

Once you have created all of your filters and a user tries to go to a blocked site they will get a message telling them it is blocked and why. This is the standard message they will get.

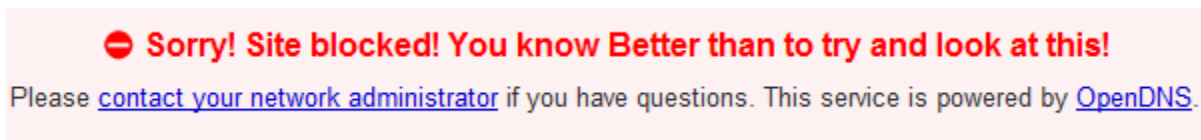


Site blocked. browseusers.myspace.com is not allowed on this network.

This site was [categorized](#) as:
Chat, Dating, Instant messaging, Social networking, Video sharing, Webmail, Music

[Questions?](#) [Not properly categorized?](#)

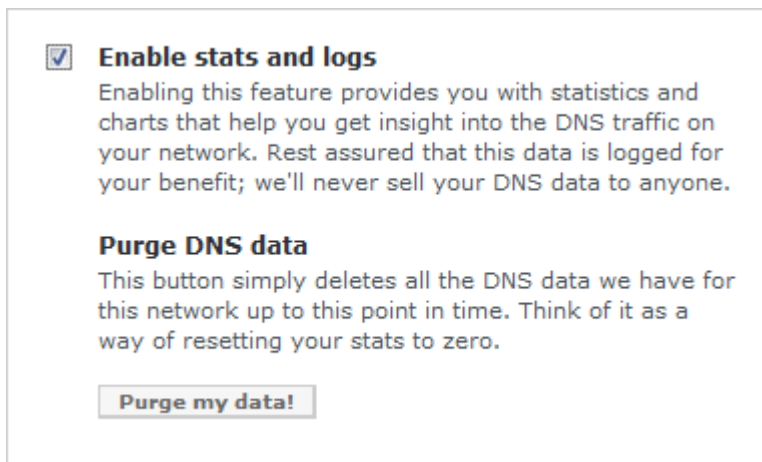
Another cool feature is the ability to customize the message the user sees. You can customize it with say your company logo or a picture of yourself. So if you child tries to go to a pornography site and they see a picture of their parent ... well ... that might urge them to never try that again! This is an example of a custom message I made.



Sorry! Site blocked! You know Better than to try and look at this!

Please [contact your network administrator](#) if you have questions. This service is powered by [OpenDNS](#).

You can also get statistic logs which will show you what type of traffic was blocked and other stats to allow you to better filter content.



Enable stats and logs

Enabling this feature provides you with statistics and charts that help you get insight into the DNS traffic on your network. Rest assured that this data is logged for your benefit; we'll never sell your DNS data to anyone.

Purge DNS data

This button simply deletes all the DNS data we have for this network up to this point in time. Think of it as a way of resetting your stats to zero.

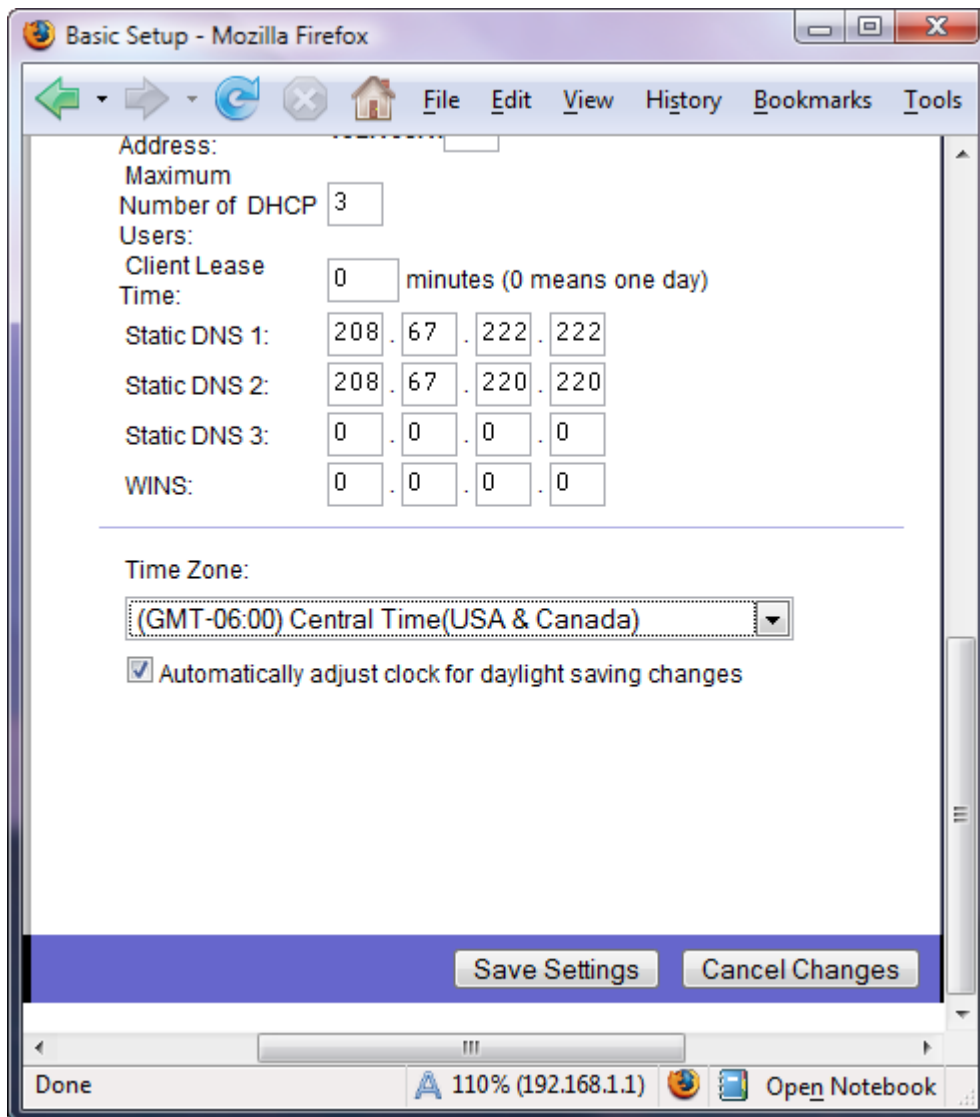
[Purge my data!](#)

OpenDNS is a great way to protect your kids from undesirable Internet content but that is not all. Businesses can definitely use it in the workplace. I personally use it to improve my Internet experience. In future articles we will be covering a lot more on this incredible web service! To get an idea of how popular, effective, and trusted OpenDNS is you can check out a list of their [business customers](#).

[OpenDNS](#) is an incredible alternative to your ISP DNS server. Simply put DNS (Domain Name System) translates IP address to easy to remember hostname's. Not only will OpenDNS make your browsing faster, there are a lot of [additional features](#) provided by this free service.

OpenDNS is free with no software to install. It also has a bunch of features such as Phishing protection, Domain Blocking, Adult Site Blocking, Typo Correction, etc. If you are behind a router the easiest way to ensure every computer on your home network is using OpenDNS is to add it to your Router.

Open your web browser and go to your router's address. Usually it is 192.168.1.1 type in the user name and password to access administrator settings. For this example I am using a Linksys WRT54GS, yours maybe different but the entry is basically the same. Under basic setup find your routers static DNS settings. Type in *208.67.222.222* and *208.67.220.220* hit save and you're done!



I highly recommend trying OpenDNS. I have been using it for over 6 months now, and in fact I forgot I was using it until I mistyped a URL and OpenDNS told me that I was accessing a shady site.