

Protecting Your Family/Employees From Internet Threats

Introduction

Protecting your home and/or business computer network from Malware is critical. One wrong click and Pandora's box could open right in the middle of your network with lots of bad consequences. After working in the technology business for over 20 years, I have seen it happen countless times. Computers infected so badly the only recourse is to wipe their hard drive and reload the operating system - always a costly option, if not in dollars, but always in lost time. To make things worse, these computers usually had some sort of anti-virus software loaded on them as well, but did nothing to stop the attack.

In this paper, I am going to share a simple and FREE solution - OpenDNS.com - to help you protect your entire network: home or business from websites that intent to do harm to your computer infrastructure.



The Problem

End-users that have unrestricted access to the internet have access to potentially damaging content. This content can be damaging to the computer itself, in terms of downloading Spyware/ Viruses/Trojans. The content could also be damaging to the individual in terms of the type of content being viewed: pornographic, phishing schemes, and social networking websites can be dangerous to younger users and stealing productivity from employees.

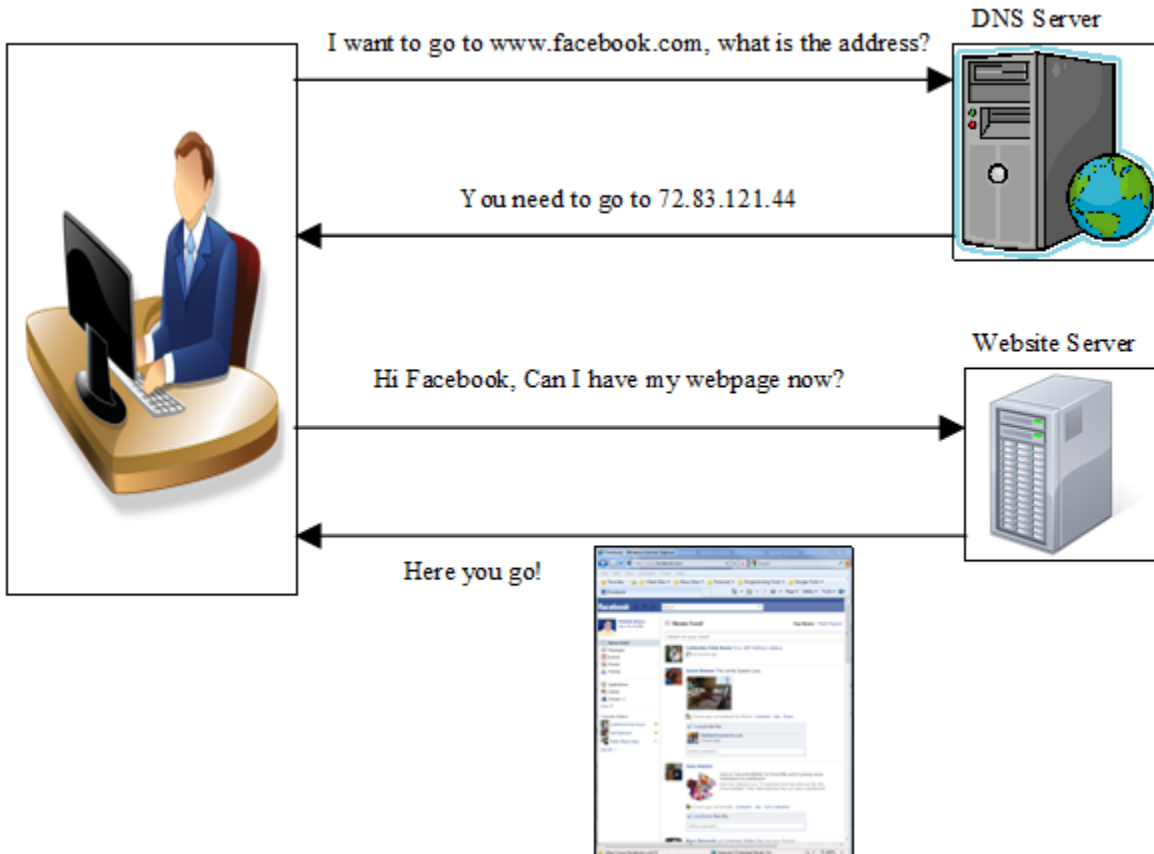
The Solution

Control user's access on the internet by implementing OpenDNS.com's DNS restrictions on your home or business network. In most cases, it can be configured in less than an hour. Once OpenDNS is operational, you will be able to choose which sites to block based on the category of those sites or select preset security levels to protect your network from known risks (see figure 2). This will prevent end-users with poor browsing habits from accessing sites that can be unproductive or inappropriate. Exceptions can also be set for specific sites.

For example, If you block a category like Social Networking, but you genuinely use FaceBook for business purposes, you can create an exception of domains that never get block regardless if their category is blocked. The converse is also true, you may decide not to block any category, but notice that employees are wasting time on a few sites like EBay or YouTube, you can block access on a site-by-site basis to prevent access to those sites from your network.

How does this work? The answer is DNS (Domain Name System). Simply put, when you type a website into your browser like www.google.com (a URL address), your computer goes out to a DNS server to retrieve the numeric address of www.google.com so that your computer can talk to that site.

Figure 1 - Steps taken when a user requests a website



In most circumstances, you would use the DNS servers provided by your Internet Service Provider (AT&T, Time Warner, etc.). These DNS servers are typically 'wide-open' which means they resolve any URL address that is requested - good or bad. By replacing your current DNS servers with OpenDNS servers, you can selectively block requests to sites that are restricted. Instead of resolving the address of a restricted site, OpenDNS will direct the browser a page that tells the user that this site is being blocked by the network administrator.

Figure 2: Selecting the categories to block from your network or using a preset filtering level. Notice the ability to 'Always Block' or 'Never Block' below to create a list of exceptions.

Web Content Filtering

Choose your filtering level

- High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. 26 categories in this group - [View](#) - [Customize](#)
- Moderate** Protects against all adult-related sites and illegal activity. 13 categories in this group - [View](#) - [Customize](#)
- Low** Protects against pornography. 4 categories in this group - [View](#) - [Customize](#)
- None** Nothing blocked.
- Custom** Choose the categories you want to block.

<input type="checkbox"/> Academic Fraud	<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 checked="" type="checkbox"/> P2P/File sharing	<input type="checkbox"/> Parked Domains
<input type="checkbox"/> Photo sharing	<input type="checkbox"/> Podcasts	<input type="checkbox"/> Politics
<input checked="" type="checkbox"/> Pornography	<input type="checkbox"/> Portals	<input checked="" type="checkbox"/> Proxy/Anonymizer
<input type="checkbox"/> Radio	<input type="checkbox"/> Religious	<input type="checkbox"/> Research/Reference
<input type="checkbox"/> Search engines	<input checked="" type="checkbox"/> Sexuality	<input type="checkbox"/> Social networking
<input type="checkbox"/> Software/Technology	<input type="checkbox"/> Sports	<input checked="" type="checkbox"/> Tasteless
<input type="checkbox"/> Television	<input type="checkbox"/> Tobacco	<input type="checkbox"/> Travel
<input type="checkbox"/> Video sharing	<input type="checkbox"/> Visual search engines	<input type="checkbox"/> Weapons
<input type="checkbox"/> Webmail		

Looking for [security categories](#)?

APPLY

Apply to all networks

Manage individual domains

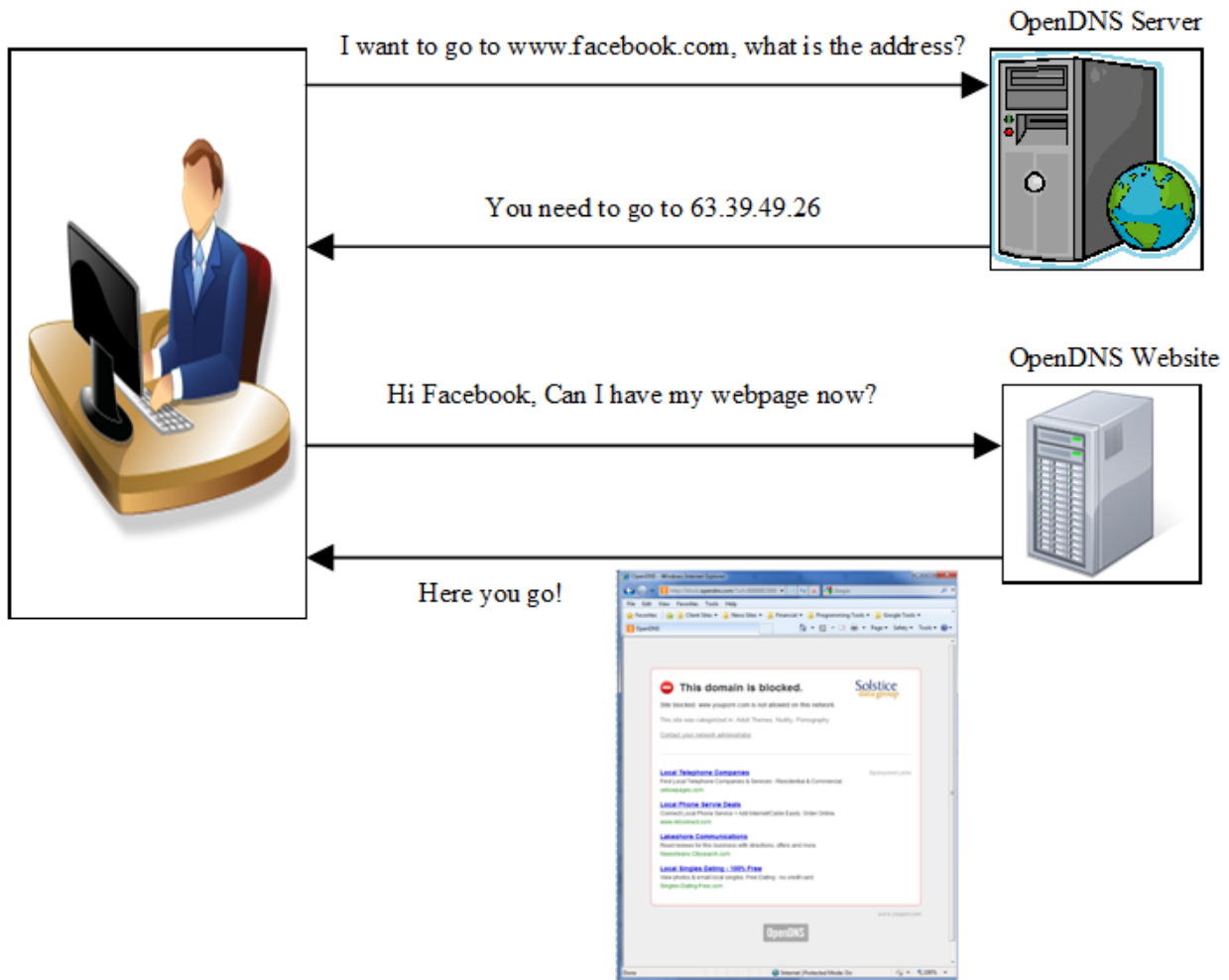
If there are domains you want to make sure are always blocked (or always allowed) regardless of the categories blocked above, you can add them below.

Always block

ADD DOMAIN

Add to all networks

Figure 3 : Process to block a restricted website with OpenDNS.com



As you can see, the browser does not know that the address (63.39.49.26) is not the 'true' address of the requested website. It's only job is just to go fetch the webpage at that address and display it. Blocked sites are redirected to an OpenDNS website that returns a 'blocked' page that can even be customized with your company logo.

Notice the four ads on the 'blocked' page that is returned to the user - that is how OpenDNS is able to provide the service for free. They do have paid plans that do not return these ads if that is something that your organization needs.

Step-by-Step Installation

- 1) From the network you want to protect, go to www.OpenDNS.com/start. You have to be physically on the network you are going to protect when signing up for your account.
- 2) Select the package that best suits your needs. Most small businesses and home based users will be fine with the Basic Package that is free of charge. Large companies may want to consider the Deluxe or Enterprise package depending on their needs.



The image shows three pricing cards for OpenDNS. The first card is for 'OpenDNS Basic', which is marked as 'FREE' in a green banner. It lists features: Reliable DNS Infrastructure, Web Content Filtering, Basic Customization, and Typo Correction. A 'Sign Up' button is at the bottom. The second card is for 'OpenDNS Deluxe', starting at US \$9.95/year. It lists features: Reliable DNS Infrastructure, Web Content Filtering, Advanced Customization, and Whitelist-Only Mode. A 'Buy Now' button is at the bottom. The third card is for 'OpenDNS Enterprise', starting at US \$2,000/year. It lists features: Reliable DNS Infrastructure, Web Content Filtering, Malware Site Protection, and Delegated Administration. A 'Buy Now' button is at the bottom.

- 3) Click on 'Sign Up' and create your new account. OpenDNS will send you a confirmation email to activate your account, so be sure that the email address you use to create your account is a working address.
- 4) Once you create your account, you will see detailed instructions on how to update your DNS server info for your computer, router, or server. This is probably the trickiest part of the installation procedure and you may want to consult with an IT professional if you are not comfortable. Businesses with servers need to be especially careful when making these updates as DNS can be served from the router or a server depending on how the network was designed. Their instructions are very detailed for a wide number of devices.

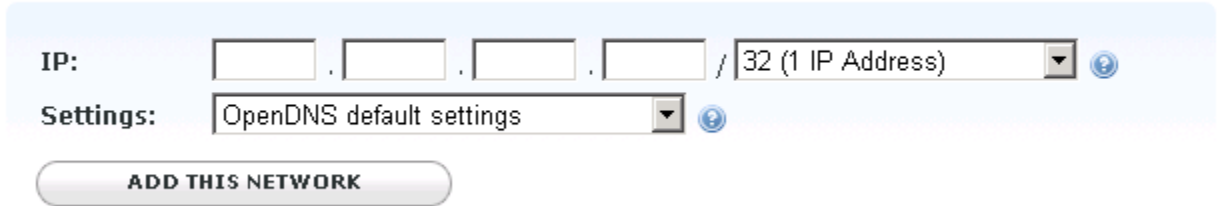
Home Users: Most home users will select 'Router' to change their DNS info in their router thus making all device in the home connecting to the router subject to the restrictions setup in the OpenDns account. If you only have one computer at home, you can select 'Computer' and just change the DNS info on your computer to start using OpenDNS.

Business Users: More than likely, you will either choose 'Router' or 'DNS Server' to update your DNS info. This will update all the computers in your organization that connect to the router or server to force them to use OpenDNS and thus protect them.

OpenDNS servers are located at 208.67.222.222 and 208.67.220.220.

5) The next step is to add your network to your account. Click on the 'settings' tab and you should see a box like the one below populated with your IP address.

Add a network



If you have a dynamic IP address, you will need to make sure that you check the 'Dynamic IP Address' box. Most DSL and Cable customers will be a dynamic IP address. You will need to install the OpenDNS client software on your PC or better yet, configure your router to report your IP address to OpenDNS as your IP address changes. This is essential to provide that your IP address is up-to-date so that the your blocking configuration is enforced.

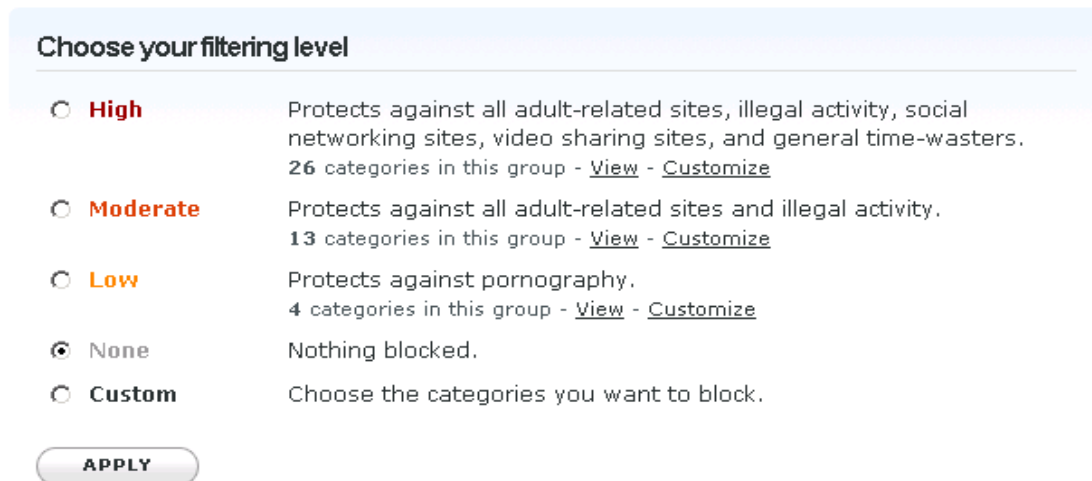
6) Once your network is added, it will be displayed in the 'Manage Your Networks' box.

Manage your networks [\(click on a label to edit\)](#)

LABEL	IP	STATS
Home	71.75.201.32	 

7) Click on the 'IP address' to setup the block policy. From here you can select a preset level of Web Content Filtering or just 'Custom' to select various categories to block. Moderate blocking is usually a good default.

Web Content Filtering



8) Configure any websites that are always allowed or always blocked. Simply enter the URL of the website (ie. www.yahoo.com) and choose whether to block or allow access from the dropdown. Click 'Add Domain' to save your selection.

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.

Always block

ADD DOMAIN

9) Enable Stats (Optional) - Click on the 'Settings' tab and find the your network listed under the 'Manage Your Networks' header. Click on the 'Stats' icon to the right.

Manage your networks [\(click on a label to edit\)](#)

LABEL	IP	STATS
Home	<u>71.75.201.32</u>	 <input type="checkbox"/>

You will need to click on the 'Enable Stats' checkbox and click Update to enable Stat Tracking. This is an extremely valuable feature that allows you to see what sites are being requested from your network. Even if you are not blocking sites from your network, you can see what sites are the most popular with your network users. OpenDNS will even alert you on the dashboard if Malware activity is detected:

Malware/Botnet Activity Detected

Need help? Read our [malware FAQ](#).

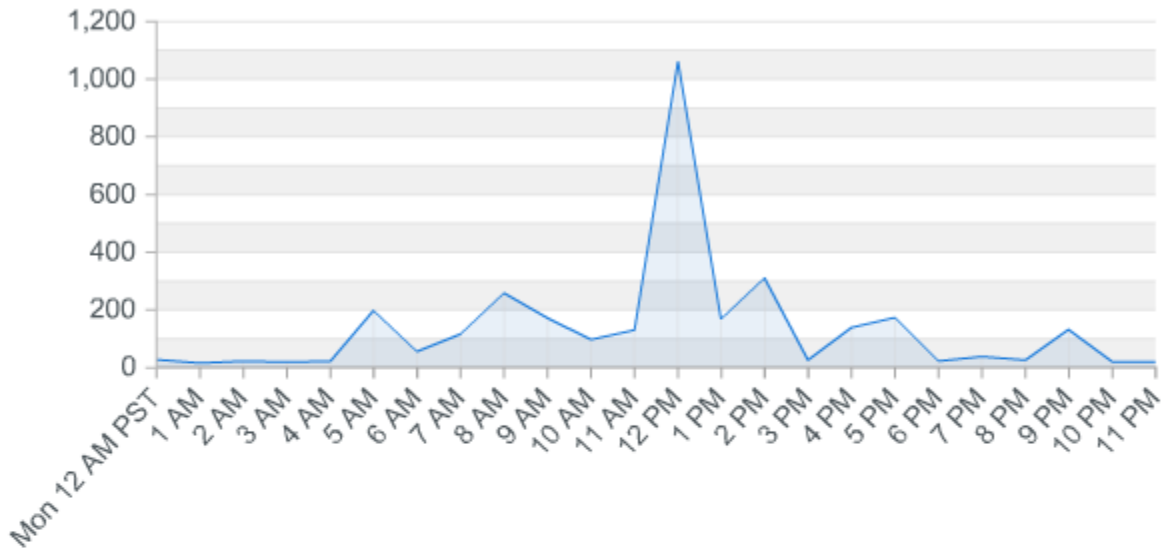
ACTIVITY	LABEL	IP	STATS	LAST SEEN	HIDE
Malware	Home	71.75.201.32		Feb 9, 2:17pm PST	

This is determined if there are many sites are being called from your network that are associated with Malware/Viruses destinations.

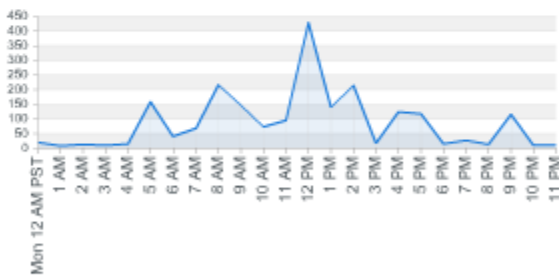
You can login to your OpenDNS.com account to check your stats as often as you would like.

Here is an example of a stat snapshot. You can drill down into the details of any category over any time span to get great reports about the activity on your network.

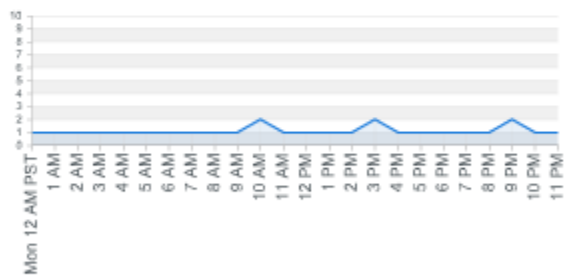
Recent Activity (all your networks, last day)



Unique Domains



Unique IPs



Request Types

Type	Requests
A	3287
PTR	35

Top Domains

Domain	Requests
checkip.dyndns.org	131
safebrowsing.clients.google.com	77
sip1.ringcentral.com	49

With Stats enabled, you can see all of the URL's that your users are calling - those that are blocked and those allowed.

Conclusion

While there is no one single bulletproof security software or hardware to protect your network from the many threats roaming on the Internet. Using OpenDNS.com in conjunction with a good anti-virus (like Trend Micro) and an email spam-filter solution (like Exchange Defender or Appraver) is a comprehensive approach to protecting your network and it's users.

In a home network setting, blocking pornographic , adware, peer-to-peer file sharing, and phishing sites - you have just dramatically increased your chances of not getting some type of malware onto your computer.

In a business environment, increasing the blocking to include non-productive social networking and instant messaging sites can significantly decrease the amount of time wasted by employees.

OpenDNS.com gives you the flexibility to manage the blocking policy that works for your situation.

Written By Patrick Arney
Solstice Data Group
February 12, 2010
patrick@solsticedatagroup.com