Internet Filtering with OpenDNS

Almost all libraries within our state offer one or more forms of internet access as a service to anyone entering its doors and, sometimes, to people who only hover near the periphery, taking advantage of a wireless signal that expands past the walls of the library to the steps and streets outside. For libraries who are part of the Maine School and Library Network (MSLN), providing this access may mean an obligation to establish some controls over what it is used to access. MSLN has found a solution for libraries who want, or need, to manage and monitor how this public service used, and offer tools for refining the parameters of its use.

Glossary

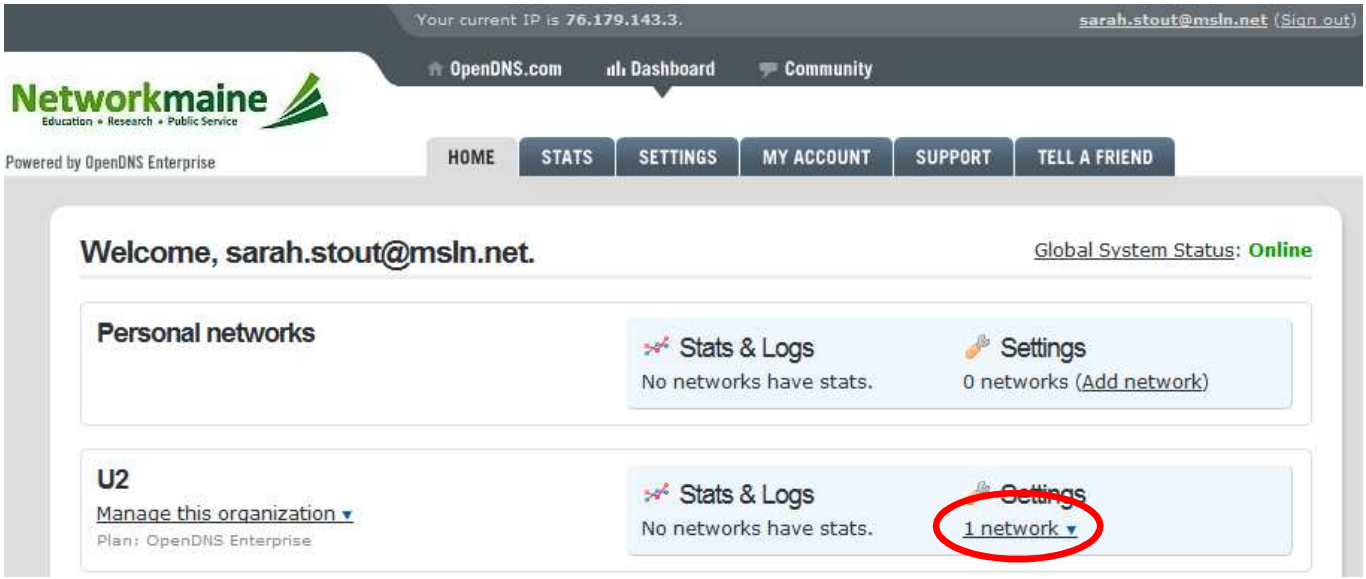
URL: Uniform Resource Locator. Sometimes called a "web address", the chain of words, letters, numbers and other symbols that help people find specific places on the Internet.
Domain: the often-recognizable "pieces" of a URL. Domains exist in levels; examples of top-level domains are .com, .org, .gov, .edu, .us, and second-level domains like google.com, nasa.gov, or wikipedia.org.
IP (Internet Protocol) Address: the "phone book" by which individual computers or networks are identified for internet traffic purposes.
DNS: Domain Name System. The Internet tool used for translating URLs (easy for humans) into IP addresses (easy for machines).
Filter: technology protection measures put in place, either on a computer or across one or more networks, to observe traffic coming from or to a network and selectively permit or block that traffic by a variety of criteria.
Whitelist: a roster of URLs or domains that are recognized as suitable by a filter.
Blacklist: a roster of URLs or domains that are recognized as unsuitable by a filter.

How to begin

This tool is for libraries wanting to use or refine the filtering options already in place for their MSLN connection. If your library has recently joined MSLN, if you are a new technology coordinator for your library, or you have forgotten your username and password, you should call MSLN at 1-888-367-6756 or email support@msln.net and ask for your username and password to the OpenDNS filter.

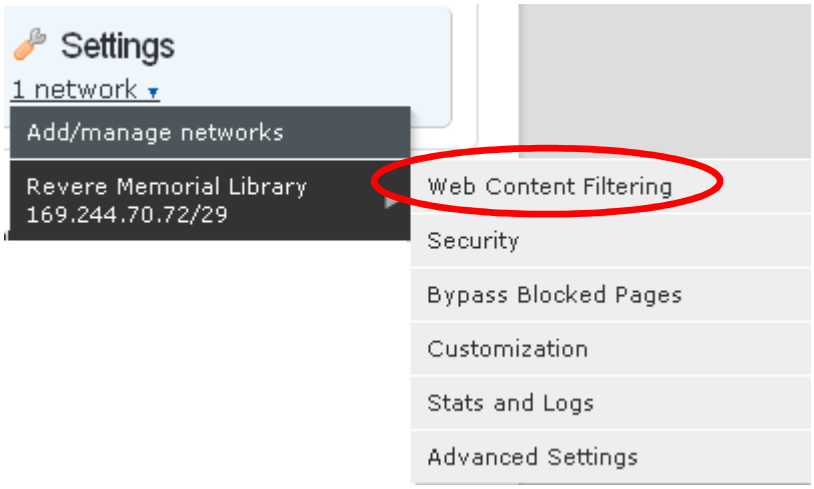
Start by going to the OpenDNS page at: https://filter.networkmaine.net and signing in.

You will now be at the OpenDNS dashboard.

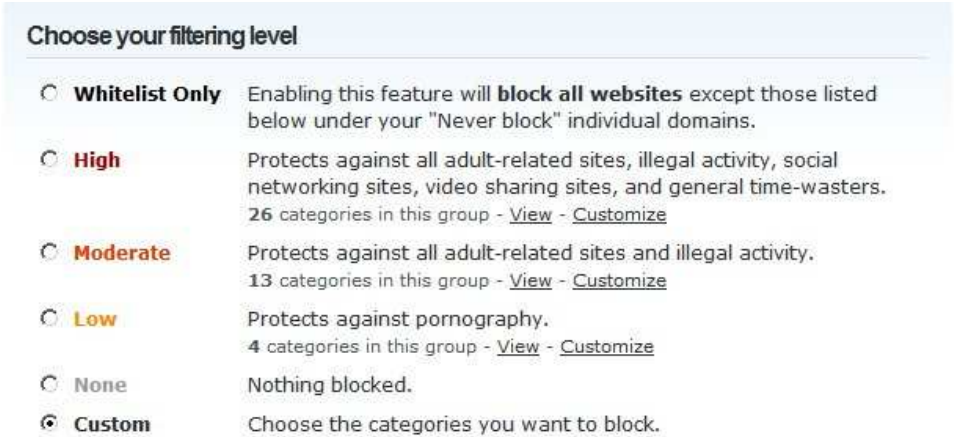


Filtering

From the dashboard, underneath the settings that correspond to your organization, click the drop-down menu arrow, move your cursor down to the library name, and then select **Web Content Filtering**.



This will bring you to the Filtering page, where you will have several options: Whitelist Only, High, Moderate, Low, None, or Custom. You can get more information about what each category will block by clicking on "View" within the category description. You may also refine each category by clicking "Customize" and choosing additional categories to be blocked, or removing categories.



Low filters: **Tasteless**, **Sexuality**, **Pornography**, and **Proxy/Anonymizer**.

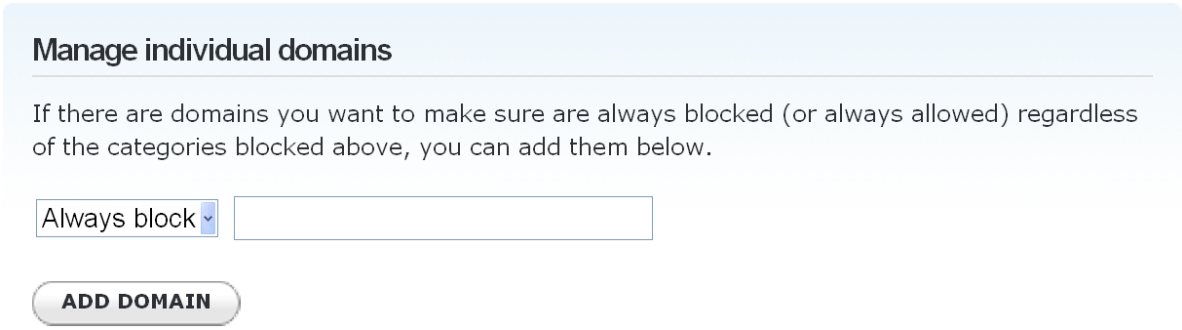
Moderate filters: everything in Low, **Adware**, **Alcohol**, **Dating**, **Drugs**, **Gambling**, **Hate/Discrimination**, **Weapons**, **Lingerie/Bikini**, and **Nudity**.

High filters: everything in Moderate, **Chat**, **Classifieds**, **File Storage**, **Games**, **Instant Messaging**, **P2P/File Sharing**, **Social Networking**, **Video Sharing**, **Visual Search Engines**, **Webmail**, **Photo Sharing**, **Adult Themes**, **Forums/Message Boards**.

The complete list of categories is:

Brief descriptions of each can be found by hovering the mouse pointer over the name of the category. You may also check to see whether specific domains are filtered, and within what filtering categories they fall, by clicking on the Find Out link under “Check a domain”.

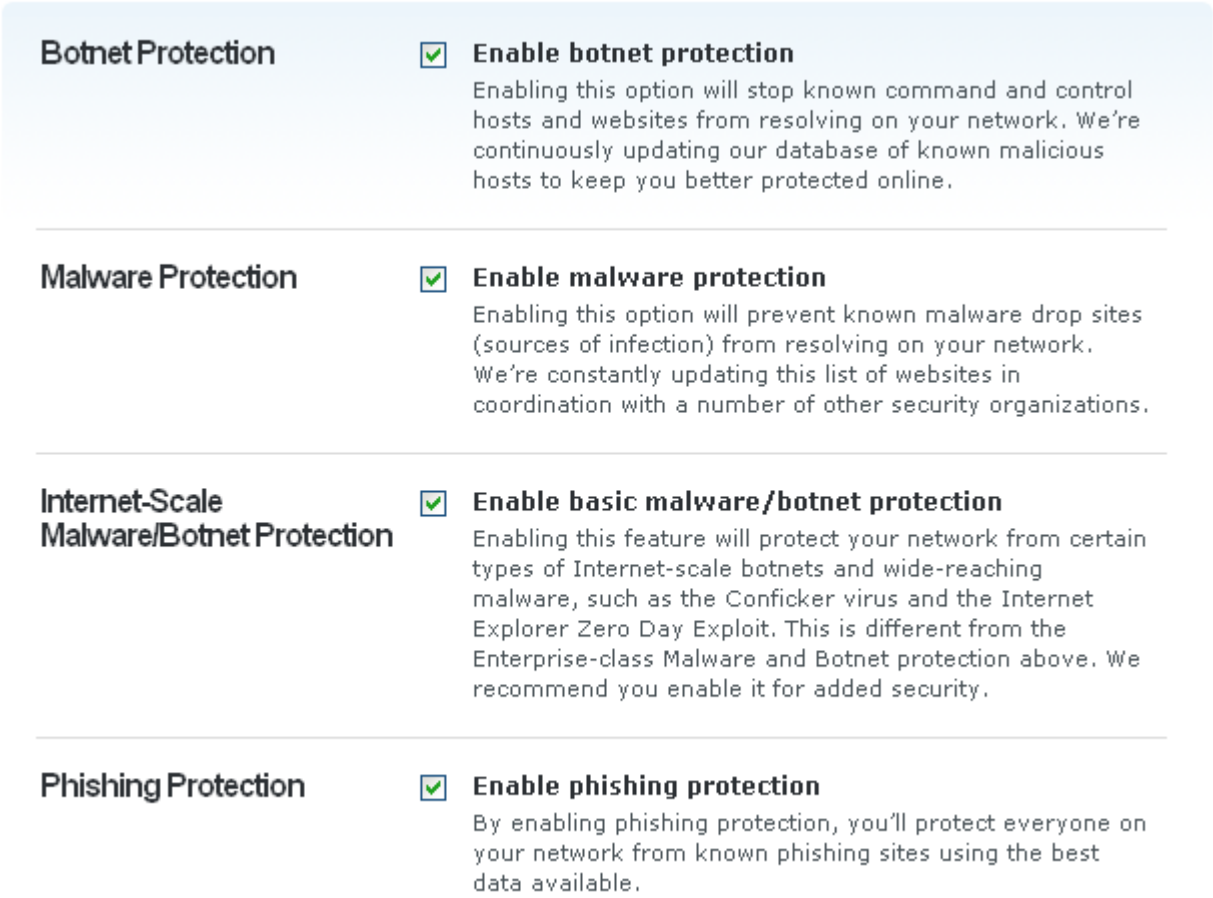
You may also add specific domains to your Blacklist or Whitelist if you choose.



It’s important to note that not all the categories refer to content. Some of the categories attempt to address potential avenues to objectionable content by filtering services or the nature of traffic. Examples include Proxy/Anonymizer and P2P/File Sharing. There are also security options that can work with filtering categories to provide additional protection for your library resources.

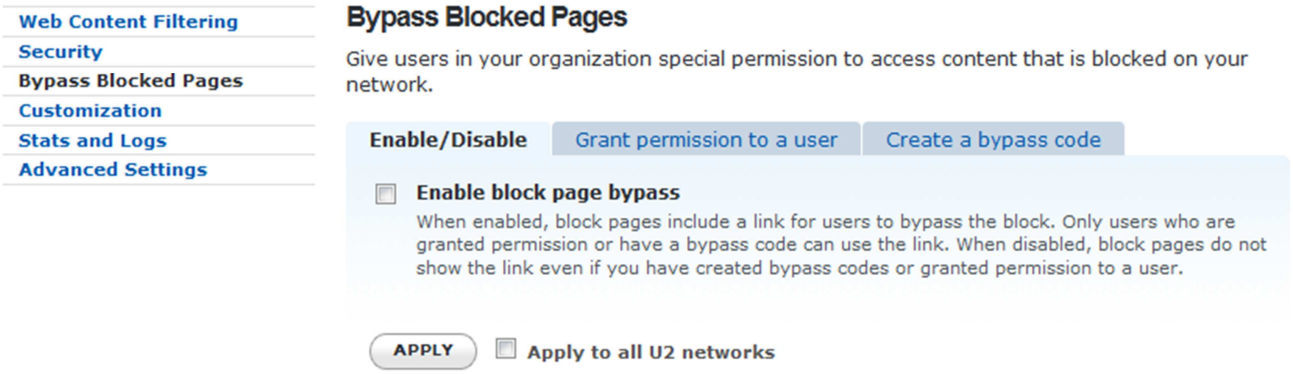
Security Resources

As safeguards against malicious software or hosts, choosing to enable these options will greatly reduce the vulnerability of a network.

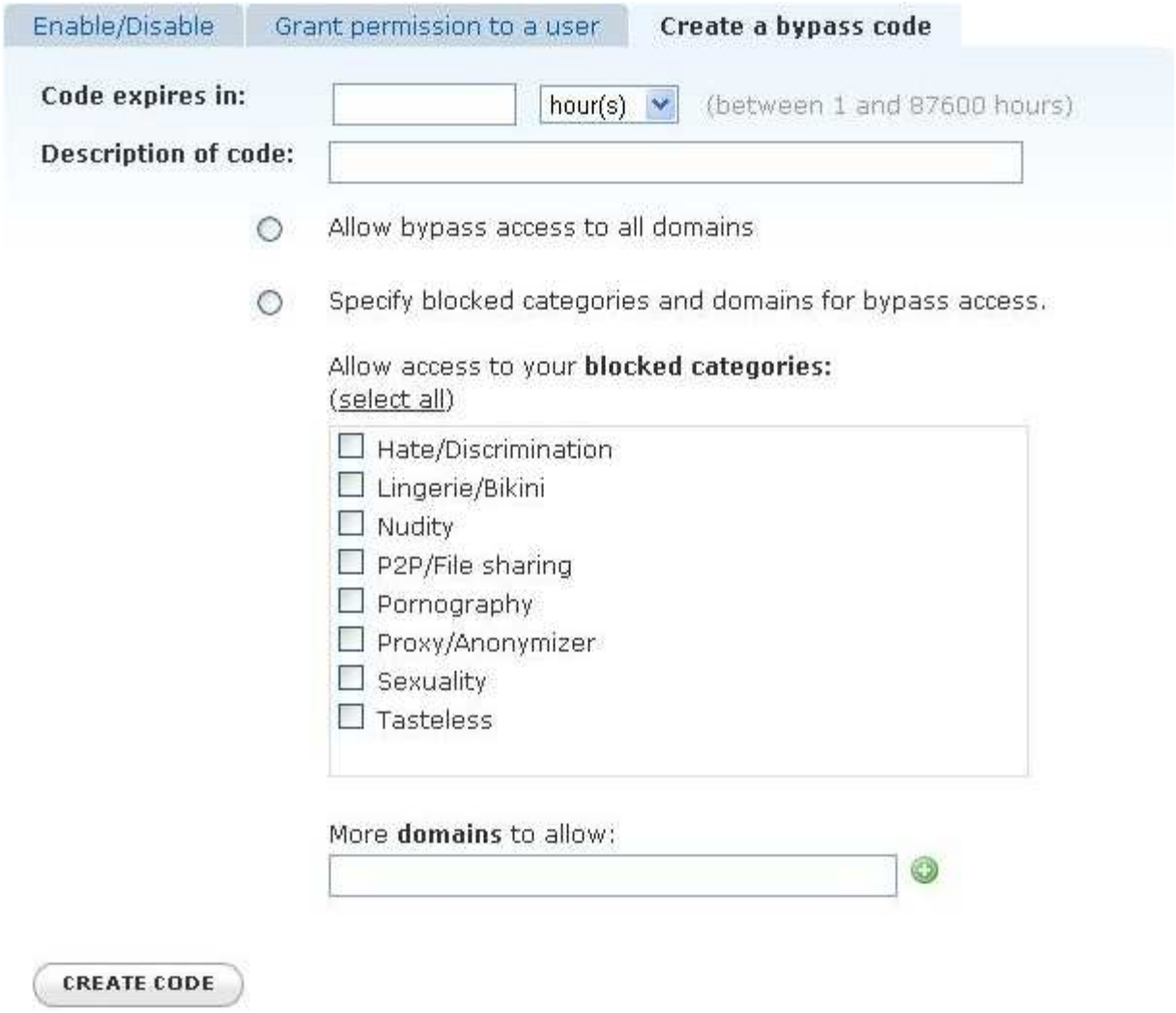


Bypassing the filter

To configure bypass options for your filter, select **"Bypass Blocked Pages"** from the left menu or the dashboard settings drop-down menu. There are two ways to bypass a blocked page: by authenticating as an OpenDNS user in the blocked page bypass options, or entering a pre-created bypass code. First, you must check the box named **Enable block page bypass** before blocked pages will provide a bypass option.



Creating a bypass code is the best approach to meeting CIPA requirements for requesting adults to bypass the filter. Click **Create a bypass code**.



You may create a bypass code that will bypass all or any part of the existing filter, and persist for anywhere between one hour and ten years. A bypass code consists of five random alphanumeric characters. If you are providing patrons directly with the bypass code, it is advised to create codes of shorter duration. If a staff member is handling the bypass directly (and being careful with keeping the bypass code private), then a bypass code of longer duration may be helpful. You can create multiple codes if necessary.

You may also revoke codes if there is a need. At the bottom of the bypass code page, all codes are listed, with details of what they are set to bypass, time to expiration, and a box labeled “revoke”. Check the boxes of the codes you wish to revoke and click **Revoke Access**.