

Childproofing Your Home Network with OpenDNS

The goal of childproofing your home network is to keep those using it including yourself from accidentally or purposefully viewing adult content or performing criminal acts like illegally downloading copyrighted material. Remember that if it is your name on the internet bill you are liable for everything regardless of who is downloading the illegal material.

The approach we are going to take is first we are going to do our best to block the bad content and log all traffic so that we can keep tabs on what is going on. Next, we are going to do our best to stop people from getting around those road blocks. Finally, we are going to secure our network so that we can control who has access to our internet connection. In addition to these steps, we recommend placing your computer in a high traffic area in your house if possible. Obviously this may not be feasible for laptops, but it will significantly reduce the opportunity for others to sneak behind your back and to use your computer in ways you do not want them to.

Step 1: Use OpenDNS

When you browse the internet your computer uses what is called a Domain Name System (DNS) to navigate the web. Think of DNS servers as giant yellow books. Most likely you are using the servers provided by your Internet Service Provider. It is better to use OpenDNS as that will allow you to trim down the yellow pages removing all of the sites with the bad content. It will also track what sites people are visiting. As a side note, OpenDNS has proven to be faster than other DNS servers and they have been quicker to fix security flaws. To use OpenDNS we need to do the following.

1. Browse to www.opendns.com.
2. Create an account.
3. Use the Settings tab to filter the web. Note they provide a few simple options or you can get more fine grained control.
4. Under the settings tab you will find a link to free software to keep your IP address up to date. Install this software.
5. If you have a router that allows several computers to get to the internet you will need to update your router settings (this will be different depending on the router you have). This is the most difficult step, but it is necessary.
 - a. Set your router to use the servers 208.67.222.222 and 208.67.220.220 for DNS.

Step 2: Deny Administrative Access to All Others

If others can install software and/or change the computer's network settings they can get around every road block we put up and they will be able to cover their tracks. Unfortunately you cannot properly do this on Windows XP and will need to have at least Windows Vista, Windows 7, or OS X.

To do this you must create a separate user account for everyone and password protect your account. Open the control panel and open the User Accounts program. You can create new users here. Set yourself up as an administrator and set everyone else up as a standard user. Now when others want to

install software you will need to go over and enter your password. It may be a pain, but you are now in control of the computer and can monitor everything others do.

You may also want to check out the parental controls in Windows Vista and Windows 7. Also, Windows provides a public folder under C:\users. This is where you will need to put stuff like music and pictures that you want all users to share. While you as administrator will be able to view everyone else's files they cannot view yours and if you have several kids they will not be able to view their sibling's files.

Step 3: Password Protect your Wireless Router

If you have a wireless router you should create a password for it. You will need to pull out your instruction manual for configuring the router. Once you figure out how to get to the administrator panel of your wireless router you should first change the admin password for the router if you have not already done so. The default passwords that routers are shipped with are well known and published on the web. This is good if you have to reset your router or cannot find the instruction manual but also bad as your neighbor or kids can easily monkey with your router if you do not change the password. After you've set the router password you should configure the wireless network to use WPA2 and create a password. Do not use WEP as it is easily hacked. We recommend using an easy to remember phrase with some form of punctuation in it. This will make it hard to crack, but easy to remember and hand out to your friends.

Step 4: Monitor Your Network Traffic

If you've followed the above steps congratulations. You now have a really secure network and have made it extremely difficult for people on your network to view adult content or download copyrighted material. Unfortunately security holes are found all the time and no method is fool proof. We still recommend periodically logging in to OpenDNS and perusing the logs to see what websites people are browsing on your network.

Happy Computing

The MBC Geek Squad