Internet Filtering Basics

HighStreet

Love God. Serve People. Reach the World.

Executive Summary

For those who are busy, know technical "stuff," or just want a short answer to the question "How do I provide safe Internet access?" here are the recommendations:

Windows - http://www.hedgebuilders.com/
Mac - http://www.intego.com
Smart Phones - http://www.x3watch.com
Router level protection - http://www.opendns.com

If you want more details, read on.

Why Filter?

Would you allow your child to enter an adult video store (supervised or not)? What about a store that sells questionable merchandise? If you allow Internet access in your home without providing a filter and supervision, you may be doing just that!

The Internet has been likened to the old Wild West. That analogy is fit, but the modern Internet is probably even more dangerous. When surfing the Internet, it is not always enough to just stay on safe sites. Even those sites can be compromised and cause serious problems with your computer.

Unfiltered Internet access is dangerous because of viruses, malware, spam, phishing, trojans and more. Pornography is a few clicks away; so is access to explicit sexual books and articles, how to roll your own marijuana joints, gambling, academic papers for sale, and more. Another danger is someone using your network to engage in illegal activity with you the unwitting target of an investigation by the authorities.

The steps you need to take in your house are simple but even doing this is not a replacement for effective parenting and proper accountability.

1. Talk with your family about why setting up a filtering system in your house is important.
2. Establish guidelines for when and where Internet access will be allowed.
3. Keep computers in a common place in your house.
4. Consider setting time limits for Internet use.
5. Install software to track and/or filter access to the Internet.
6. Be sure those who struggle with visiting inappropriate websites are NOT the ones with the control of the software.
7. Talk with your family regularly about what they are viewing and doing online.

There are a few different ways you can filter internet access. There are pros and cons to each, and the best solution is often a mix of more than one type of filtering.

Client Based Solutions

A client is simply the device you use to connect to the Internet. Today, clients can be smart phones, tablets, desktop computers and laptops. The advantage to installing software on a device is clear - no matter where the device goes, filtering is a part of the package. Different options exist, depending on your device. Some filter and prevent access to websites, while others simply track and report.

Hedgebuilders

Client based, must install software. Comprehensive filtering. Access lists managed by them. Annual fee.

For those running Windows, this is the best filter we could find. If you try to disable it (be deleting files, etc.) all access to the Internet fails. In order to uninstall the software, even an administrator must call the company and get a code.

http://www.hedgebuilders.com/

Built-in

Client based, must configure software. Limited scope for filtering. No fee.

Both Mac and Windows operating systems have built-in parental controls. To find out more about these, check their sites:

Mac (Mountain Lion) - http://support.apple.com/kb/PH11354

Windows (Windows 7) - http://windows.microsoft.com/en-us/windows7/products/features/parental-controls

Intego

Client based, must install software. Comprehensive filtering. Access list managed by them. Annual fee.

Mac only solution. Requires administrator privileges to install. Can require a separate account to manage the filter and access settings.

http://www.intego.com

X3Watch

Client based, supports multiple device types (smartphones, tables, computers). Site tracking is free; filtering has a fee.

Supports multiple operating systems and device types. Allows you to send an email report of your activity to an accountability partner.

http://www.x3watch.com/

Summary

Based on the experience of the technology team at High Street, if you have Windows, we recommend Hedgebuilders. It is the most comprehensive and difficult to bypass of any solution tested. For a Mac, Intego is a good solution. If you want just web site tracking, without filtering, then X3Watch is a good solution. We also recommend you implement a router based solution, since it is free and is an additional layer of security for your home.

Router Based Solutions

If you have more than one computer connected to the Internet at home, then you probably have a router. This devices takes the information you request, and as its name implies, it "routes" the data between you and the final destination of your request. If you have more than one device at home, it is best to have router with a firewall.

When a request is made for a particular website, the service called DNS translates the name (www.highstreet.org) to a number that Internet devices use

to transmit information. A standard DNS service will look up the name of your website, return the number, then your browser will connect to that site and you can "surf" it. There are some companies that will provide you with DNS service and because all requests for traffic go through them, it effectively allows you to filter all requests. So, the search for a porn site will be blocked but a legitimate site will be allowed.

This service is good because it protects all devices connecting to the Internet through your equipment. If anyone without a filter on their computer used your Internet connection, they too would be protected. This is important because if someone at your location is breaking the law, you may get an unwanted visit from authorities!

OpenDNS

Free DNS services. With an account you can setup detailed filtering for your home.

Most routers allow you to change the DNS information easily. One exception is AT&T's U-Verse. In order to implement this system with U-Verse you must purchase an additional router besides the one they lease you.

http://www.opendns.com/

Details...

Definitions

Browser - software to allow properly formatted information on the web to be viewed; e.g., Firefox, Safari, Internet Explorer.

Content filter - software that manages access to information based on content, URL, IP address, etc.

DNS - Domain Name System; the servers that translate your name request (www.highstreet.org) to an IP address 69.89.31.167. More details at http://en.wikipedia.org/wiki/Domain_Name_System.

Firewall - software that prevents or manages traffic flow.

HTTP - Hypertext transfer protocol; this is the language used to transmit most web pages.

IP (Internet Protocol) address - this is the number every device connected using TCP/IP must have in order to operate. Think of it as a telephone number, only more complex. Currently, the Internet is using IPv4 but with a limitation of just over 4 billion public address. With the rise in Internet connected devices over the last 2 decades, there are not enough addresses to go around. Since 2006, corporations and ISPs have been implementing IPv6, which allows for many more devices - 3.4×10^{38}. (That's around 7.9×10^{28} or 79,800,000,000,000,000,000,000,000,000 MORE than IPv4).

Router - device that manages traffic flow between two networks.

SSID - service set identification; this is the name your WiFi router broadcasts to those seeking a connection.

URL - uniform resource locator - for example, www.highstreet.org/messages is a URL. More details at http://en.wikipedia.org/wiki/Uniform_resource_locator

More Details about Content Filtering (for those who are interested)

Content filtering can be done based on a number of criteria.

- URL blocking: The URL of known bad sites will be blocked.
- Keyword blocking: Any pages with one (or more) keywords will be blocked.
- Weighted phrases: Weighted phrase limiting prevents/allows a page based on the context of the content. For example, the word "breast" might be used properly, or improperly. If a weighted phrase limit is exceeded, it means too many inappropriate words appeared and the page won't load.

Many companies that provide filtering track and categorize websites so that when you choose what you want to prevent/allow on your network you just check a few boxes and they take care of the rest.

The Big Picture

None of these solutions is perfect. A combination approach to securing your systems is best. A knowledgeable technologist (or a persistent teen) could potentially bypass these measures. Ultimately, the best approach is holistic; communication, accountability and limited access will reduce the exposure to the evil accessible on the Internet today.

Many homes today have WiFi. If you have WiFi at home, be sure it is secured. Best practices with WiFi:

- Use a hidden SSID
- Implement a password that is not easily guessed
- Use the highest security level possible - WPA2 is best.

If you need more information, use your favorite search engine and it shouldn't take you long to find what you seek.