

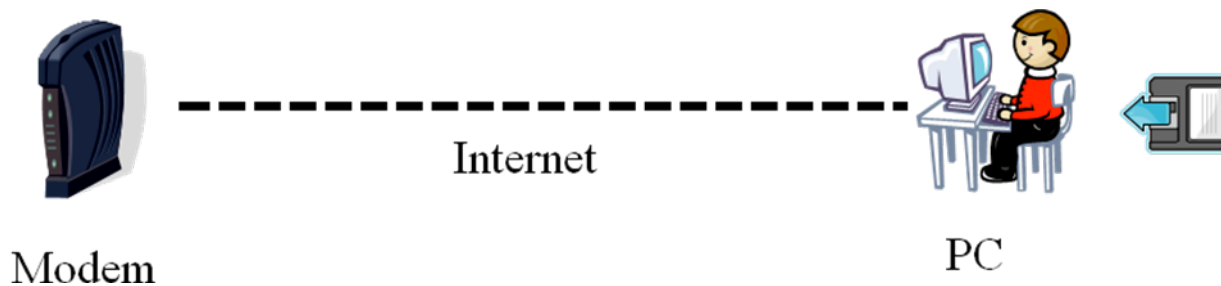
Internet Safety in your Home

Providing laptops for our students is truly a blessing. These computers have the potential to open doors of learning for our children, create additional tools for our teachers, and serve as an "education multiplier" for our school. But issuing these computers to our students is not free from peril. One valid concern is ensuring the safety of our kids in cyberspace.

The dangers are real. For example, in one study "approximately 1 in 25 youth received an online sexual solicitation where the solicitor tried to make offline contact."¹ Additionally, "only 27 percent of children who received unwanted sexual material online in that time period told a parent or guardian."² We have an obligation as parents and guardians to protect our kids to the best of our ability.

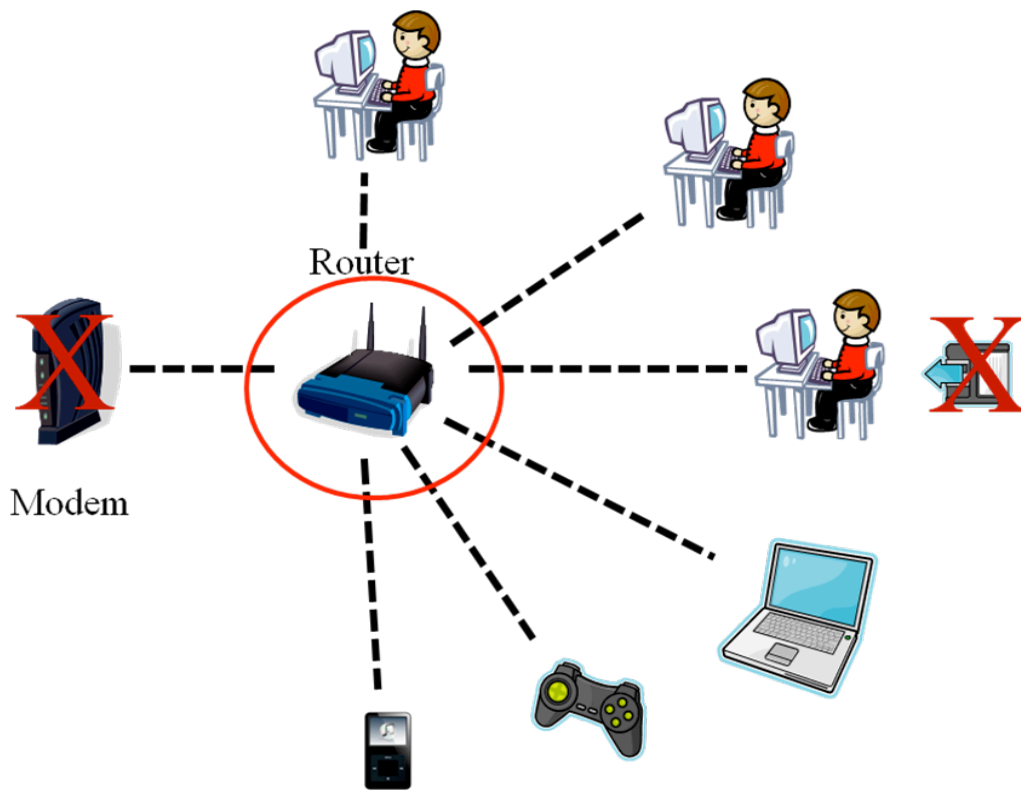
My name is Lance Schroeder. I'm a St. Mike's parishioner with children at our school. I have been asked to provide some computer safety recommendations. These recommendations will include some commercially available software/hardware products that are easy to install and manage. These are the tools that have worked for us. I don't represent any company or solution. I'm just a parent of five with an interest in keeping kids safe on the internet. I'd like to share some of the lessons I've learned.

Back when most homes had only one or two computers with only one way to access the internet (usually a modem connected to your phone line), it was relatively easy to control access to the web. Software packages, such as "Net Nanny", were available to control length and breadth of access to the internet. Internet browsers could be customized to restrict access. Even search engines had tools to limit your family's exposure.



In this simpler computer world, software or individual computer filters/settings were a logical choice. I do not have one of the proposed laptops in hand as I write this letter. It is possible that there are sufficient parental controls available on these laptops to suit most of our needs. But whether that is true or not, there are additional considerations.

Today, just about every device in the home is a conduit to the internet. From your Play Station or Wii, to your son's handheld PSP, to his friend's iPod Touch, to your student's new laptop, everything has/wants access to the internet.



In this more complex scenario, buying software to install on each device is neither cost

efficient, nor feasible. Configuring filters and/or parental controls on each device is difficult and can also have limited effectiveness (ex. setting restrictions to Internet Explorer doesn't prevent unfiltered access through a different web browser like FireFox, Opera or Safari; Configuring Google to only allow "Safe Searches", doesn't prevent unrestricted access to other search engines such as: Yahoo, Bing, Ask or Duck Duck Go!). Given these limitations, the simplest and most effective ways to address internet browsing safety seem to be at your Modem or your router.

The Modem (Cable/DSL/Phone) would be a good starting point, since it is where the internet enters your house. But most of us don't own the Modem in our home. It usually belongs to the Internet Service Provider (Integra, Comcast, etc). The ISPs that I have worked with in the past, do not allow you a great deal of control or customization of their Modems. So, the Modem is a bit of a dead end, which leads me to the router.

As I was trying to tackle this problem for my own home last year, my first attempt was to configure some of the commercially available routers on the market. I tested the parental controls on Motorola, Linksys and D-Link routers. I was disappointed with the effectiveness and functionality of these routers. These manufacturers may have added capability since I reviewed them, but at the time they were inadequate for my needs. In the end, my research led me to a router built by Phantom Technologies called, iBoss (available at <http://residential.iphantom.com/>).

Pros: The iBoss has extremely robust parental controls. You can block entire website categories (ex. Adult, Guns, Drugs, Gambling). You can block web programs (ex. AOL Instant Messenger, File Sharing programs like Limewire, or games like World of Warcraft) or you can create a schedule of when those web programs are available. You

can filter specific keywords (most of which I don't care to type here, but are all preloaded for you by subcategory that you can select/deselect). In addition you are able to block or allow specific websites. iBoss also allows you to schedule when the internet is available so you can have set downtimes, with different settings for different days. All of these parental controls can be set to apply to specific computers or individual users.

The iBoss is very easy to install and use. Once installed, all of the above features are managed from a control panel that you access from a web browser. Navigating through the control panel settings is straight forward. For example screen shots, go to http://residential.iphantom.com/ibh_more_info_screenshots.html.

Another advantage of the iBoss is that the folks at Phantom are constantly scouring the net and adding new sites to the lists of blocked categories. This fact however, leads to the router's biggest disadvantage, cost. The initial purchase price isn't out of line, at just under \$50, but to pay for the continuous updates this router requires a subscription of about \$5/month.

Cons: The largest detractor for me in recommending this router is cost. There are also some speed issues that are discussed in this CNET review:

[http://reviews.cnet.com/routers/iboss-home-parental-control/4505-3319_7-](http://reviews.cnet.com/routers/iboss-home-parental-control/4505-3319_7-33669195.html)

[33669195.html](http://reviews.cnet.com/routers/iboss-home-parental-control/4505-3319_7-33669195.html). The interesting part of the review is the comments from the parents that follow the article. The editor is critical of the cost and performance and that is his overriding concern. But the essence of the parent's comments is, "you've missed the point – parents buying this device are willing to accept these deficiencies in exchange for browsing safety."

The last "con" I'll mention is that any time you add a layer of complexity to your

computer/network you will inevitably lose some of the ease of use and flexibility that you had before. For example, you might be searching for information about “model” rockets or how best to prepare chicken “breasts” only to find out that your search has been blocked. As is true with Firewalls, which also add complexity, most of these nuisance messages will disappear over time as you “train” your router.

Limitations: Having the best controls possible for your internet connection, doesn’t stop kids from joining other unprotected wireless connections. So, if your neighbor has an open (no password required) wireless connection, and it is accessible from your home, students could bypass your restrictions.

Conclusion: As more and more “information” is available on the internet, and an ever increasing number of devices are capable of accessing that information, it is considerably more difficult to keep our kids safe. The first and most effective line of defense will always be communication with our children. No technological tool will ever relieve our responsibility as parents to instill positive moral values, openly discuss the dangers inherent on the web and identify pitfalls. Beyond that most important step there are some safeguards we as parents can put in place. Learning about, configuring and monitoring the parental controls available on individual devices, like these new laptops, is an important safeguard. But it has been our experience that these controls though important, by themselves are inadequate.

I’m certain the school will have safeguards in place for their distributing, “routing”, of internet access while the laptops are in use at St. Mikes. It is my recommendation that you establish similar safeguards at home. Although there are surely other options, for us the simplest and most effective solution has been to establish an internet content

filter using the iBoss router. I hope sharing the lessons we have learned is helpful to you.

Your friends,

Lance and Jean Schroeder

Footnotes:

¹ Source: Janis Wolak, Kimberly Mitchell, and David Finkelhor. Online Victimization of Youth: Five Years Later. Alexandria, Virginia: National Center for Missing & Exploited Children, 2006, page 37 and <http://www.take25.org/page.asp?page=55>.

² Ibid.

Reviews:

- Video Review: <http://www.youtube.com/watch?v=kpbIKsKDBS0&feature=related>
- CNET Review: http://reviews.cnet.com/routers/iboss-home-parental-control/4505-3319_7-33669195.html.
- Disney Family Review: <http://family.go.com/products/article-643798-top-hi-tech-gadgets-for-kids-t/6/>

To Purchase:

- <http://residential.iphantom.com/residential.html>