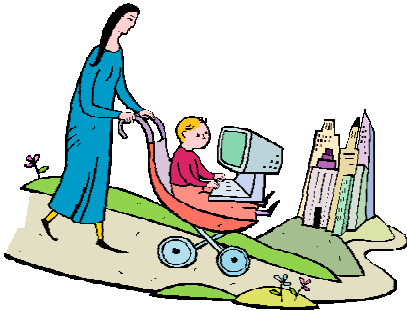


HOW CAN I PROTECT MY CHILDREN WHEN THEY USE THE INTERNET?



As early as elementary school, they use the internet at school, many of their friends have email and instant message ids – they can use it to make and contact friends all around the world. Unfortunately, others can use it to contact them too.

Pornographers, predators, spammers, supporters of everything I don't want my child to ever even hear of – is it really safe to let my kids on the internet at all?

This article gives you a quick overview of how to protect your kids from things you don't want them to see, and people you don't want them to meet while they surf the net. A condensed version of this article is available from our site as a brochure, with room on the back to include your organisation's information.

The first thing to remember is that the most important thing protecting your children is you. There are internet filters, programs that call themselves "Nanny," firewalls promise to block intruders, other programs "immunize" your system from viruses – but in the end, they can all be bypassed, disabled, or out of date. Depend on yourself and your own instincts – not automation or software. Just as you wouldn't drop your child off in a dangerous place alone, they should never go onto the net without you.

HAVE A STRATEGY

Any effective defense needs to know what it is up against. For your child on the internet, there are four main concerns:

- Avoiding undesirable content
- Blocking spam, scams and thieves
- Intercepting viruses, spyware, adware
- Avoiding predators

Obviously predators are the most dangerous, the others, however, are guaranteed to be encountered by your child. The best approach is a deep defense – in this case three basic layers – Supervision, Education and Network Security.

Each layer of the defense applies to all four threats, but they all work most effectively together.

SET THE RULES

There is literally everything to see on the 'net, so starting off by setting limits is essential. That anything which would be forbidden in print or on film is also off limits on the net is a good start – but remember that a lot of things are interactive as well. Be clear with your child where on the net they can and cannot go, and what they cannot do. Set rules about downloading files, use of email and Instant Messenger use. Find out what their friends do on the net, and make clear your rules about it.

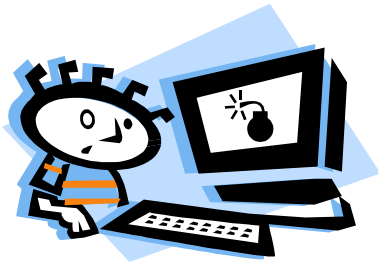
LIMIT ACCESS

There must be only one computer in your house where your children can access the internet, and that computer must be in a public area of the house. Public means the area you will be in while your children surf. This is the single most important rule in allowing your children internet access. Your child must not have internet access in their room, in the basement, or any other part of the house that affords them privacy. The issue here is not whether

or not you trust your child. Predators operate by gaining your child's trust. They do this by taking their time to establish a relationship, showing interest in the child, and sharing secrets. These things all require privacy. Having the computer where you can look over your child's shoulder any time removes their ability to get close to your child. The public location has the bonus of reducing the temptation to search for forbidden content.

FIREWALL YOUR CONNECTION

Firewalls block unauthorized traffic to and from your network. This makes it more difficult for spyware and viruses to infect your machine, and more importantly, more difficult for anyone to plant



programs on your machine to help them spy on you and your children. If you have DSL or Cable

access, most broadband routers include easy to administer firewall settings. For dialup access, software firewalls, such as Norton Personal Firewall, or Zone Alarm can do the same job. Both options are inexpensive – in fact, Zone Alarm has a free version.

BLOCK VIRUSES AND SPYWARE

Viruses can damage your system, altering or destroying some or even all of your files. Both viruses and spyware can be used to turn your PC into a 'bot' for someone else to use for relaying spam or in attacking other systems, or leave open "backdoors" for someone to access your PC directly later. Spyware can capture information about you and your child, your surfing habits, and redirect your browser to unwanted sites or open popups of unwanted sites. Your other measures will be wasted effort if a spyware program opens a pornographic site while your child is surfing. Anti-

virus and anti-spyware applications are necessary on any machine connected to the internet. Symantec has been the established leader in anti-virus software – their Norton Anti-virus can present some problems, but once setup it works very well. The free version of Grisoft's AVG Anti-virus is popular and effective as well.

For Spyware, right now (11/2005) the best choice is SpySweeper – check any review. It is easy to use, and very effective. Download the free trial from their web site.

If you purchased a system with anti-virus or anti-spyware software installed, make sure it is up to date. Virus signatures have to be updated almost daily, and most programs require a subscription to get updates. Check your documentation for what you have to do (or pay) to keep your software up to date.

WATCH WHAT GETS INSTALLED

Only install software from trusted sources, with which either you or someone you know has experience. Always read the end user license agreement (EULA). Free software sometimes includes spyware or adware, and often this is spelled out in the EULA. In other words, when you click Ok and install the software, you agree to host the spyware! Many Peer-to-Peer (P2P) file sharing programs (notably Kazaa) are infamous for the spyware bundle that comes with them. P2P downloads are also a good source of viruses and spyware – it's a good idea to tell your children to stay away from music sharing (illegal downloads) and just buy the CDs.

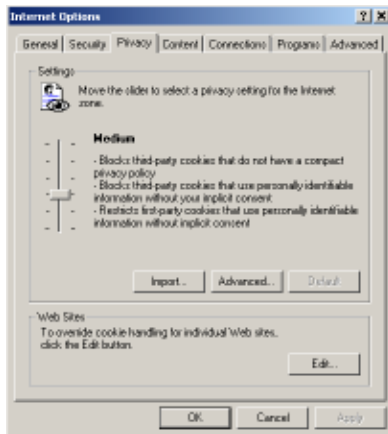
DON'T USE IE

Internet Explorer's security flaws are well documented and thoroughly exploited. [Firefox](#) and [Opera](#) are available as free downloads, easy to use, feature packed and (for now) more secure. Whatever browser you use, take advantage of its

built in privacy settings. Some key items to look for: Block 3rd Party cookies, Block graphics not from the host site (banner ads).

In IE6 Tools->Internet Options. Select the Privacy tab and make sure the slider is set to at least Medium. Under Content, you can also turn on the Content Advisor to filter content (see filters, below).

Internet settings for IE 6:



If you have Windows XP SP2 popup blocking should already be turned on. If you don't have SP2, you need to get it from Microsoft update. The install will take quite awhile, so kick it off when you're not busy. If you are using a version of IE prior to version 6, go to Microsoft Update and download the new version – it is a necessary security update.

In Firefox, choose Tools->Options and select Privacy from the toolbar. Under cookies select Allow for Originating Web Site Only. Under Web Features, select Block Popup Windows, and Load Images for the Originating Web Site Only.

Firefox's Privacy Settings:



In Opera go to File->Preferences, select Privacy, and set the cookie preferences to Do not accept 3rd party cookies.

DO USE AN INTERNET FILTER

A content filter, such as [Net Nanny](#), [CyberSitter](#) or [CyberPatrol](#), can help block unwanted web sites – some have added features such as recording IM and Chat room sessions. IE6 has a content warning feature as well, access from the Internet Options->Content tab. Be aware that content filtering is tricky – it is useful, but some objectionable content will get through, and some other items will be mistakenly blocked.

ENABLE SECURITY FEATURES

Set up your child's logon account with less than Administrative rights. This will limit them from installing programs without your permission, and helps prevent web sites from dropping "drive-by" installations of spyware on your system. Turning up the privacy settings in your browser also limits web sites ability to track your child or obtain private information from your PC.

SURF TOGETHER

The internet can be useful, informative, and a lot of fun – the safest way for your child to enjoy it is with you.

