Staying Safe in Cyberspace

by Mark Navin

The Internet is now an integral part of the culture of the developed world, but like any culture there's always a seamy side. Darker elements are only a click away. The most obvious example is pornography. The online porn industry is big business, generating more than $1 billion a year. Of the more than 1 billion Web pages on the Internet, thousands are devoted to sex in all its forms.

I am not going to debate what constitutes pornography as even legal practitioners cannot agree, but for the purpose of this article it refers to subject matter that you should have a choice to view and not inadvertently expose to minors.

With so much potentially harmful material available in one place, it's inevitable that children will stumble on such sites eventually. According to a 2002 report, nine out of 10 children aged between eight and 16 had viewed pornography on the Internet. In a majority of those cases, access was unintentional. There is technology available, however, to minimize the chances of youngsters accidentally "dropping in" on such sites.

Firewalls are a normal network security safeguard at companies nowadays. A firewall is usually a combination of hardware and software that sits between the internal network and the Internet. The most common use of the firewall is to monitor and block or allow access to the internal network from the Internet, but that is only half its job. It is just as effective in controlling who accesses the Internet and what they view.

Most firewalls contain a "context filter" that enables the network administrators to decide who gets to access what. This filter can block a host of material deemed objectionable, not just pornography. It works not unlike an antivirus program regularly downloading updated files from a central location. Text on a site a user wants to access is checked against lists of objectionable words. If nothing is found the user can surf away.

While the method can prove highly effective for businesses, a seemingly innocent word can sometimes trip up the software. Members experience one such difficulty when trying to access the Web site of a golf course in the Tokyo area that Members can use. The Club's firewall context filter was blocking the site but it was difficult to work out why. After some digging the phrase "nude greens" was discovered on the site—Japanese English terminology for open golf greens.

While most homes don't need a business-level firewall, there is a requirement for individual PC protection. Check out **http://personal-firewall-software-review.toptenreviews.com/** for a rundown of available firewalls. Firewalls for the PC are not as feature-rich as their business counterparts so sometimes other software is needed to fill the gap of the context

filter. The range of this kind of software is extensive (from site-blocking software to programs for monitoring keystrokes), but frankly much of it constitutes an invasion of privacy if installed on another machine.

A key logger (see **www.keylogger.org/**) is a program that can log everything that is typed or accessed on a particular computer, including user names and passwords, e-mail addresses and online forum messages. It can even send accumulated data to another machine using e-mail. This invasive software can be used for surveillance as it can sit undetected on a PC, only becoming visible when certain user-defined keystrokes are typed.

Information is available to anybody with access to the Internet, particularly when using an effective search engine like Google. Increasingly, Web site owners and businesses are becoming adept at working out the search algorithms of search engines and are manipulating the system to ensure that their sites end up on top of search results. Since there is so much money being generated in the online porn industry, many searches will throw up links to adult material for the most innocuous of searches.

A Google search on Britney Spears, for example, produces as hit number four a flash program debating the size of Britney Spears' breasts, which, while slightly amusing to adults, is not what most people would like their children to find when looking for information on the American teen idol. However, using **www.onekey.com/**—regarded as a child-safe search engine—the adult flash program was not listed. Onekey has joined forces with Google to weed out undesirable sites. It is a positive start for children needing to search the Internet.

While there is no need for subterfuge, there are many applications available that can protect children through site restriction and message and chat room monitoring. The site **www.edinformatics.com/internet/child_safety.htm** is a good starting point for those seeking not only software information but also help and advice. One of those mentioned is ProtectKids (**www.protectkids.com/index.html**), a site that highlights the dangers of the Internet and offers solutions. A number of excellent protection programs are available for less than $50. One popular one is NetNanny (**www.netnanny.com**), which displays statistics regarding children and the Internet as a sobering introduction.

While monitoring software is useful, it remains no substitute for parental supervision. The message should be clear: the Internet is a big place and not everyone being friendly is necessarily a friend. □

To access all previous articles, visit **www.marknavin.com/articles/**.