

Internet and E-mail Content Filtering Tools - Are they for You?

by Mike Foster

As the Internet continues to experience phenomenal growth, more and more companies are giving their employees web access at work. While the employers hope this new technology will increase sales and boost profits, the reality is that many employees are using their at-work web connection for personal use. In fact, Nielsen/Net Ratings announced that during the month of January 2000, at-work Internet users spent an average of 21 hours online, more than double the amount of time spent online by at-home Internet users.

Unfortunately, many of the employees who casually surf the Internet at work view their activities as innocent fun. After all, what harm can there be in checking a sports score or doing a little online trading? However, what these employees don't realize is the high cost their company pays due to their Internet misuse. For example, consider the small business with 15 employees, each of which costs the company \$50 per hour including overhead. If each of those employees spends just two hours per day casually surfing the net, they're costing their company on average \$1,500 per day or \$352,500 per year.

In addition to the cost factor, employee Internet misuse also accounts for 30% to 40% of lost worker productivity, according to Framingham (Mass.)-based International Data Corporation. Between visiting non-work related sites and sending and receiving personal emails, it's a wonder that some employees get any real work accomplished during the day at all.

In order to combat Internet misuse, some companies have installed Internet filtering software, which essentially blocks the employees' access to sites the company deems unacceptable. It also scans incoming and outgoing email messages for words the company finds objectionable. Those emails are then blocked so the employees can not send or receive the questionable material.

How Filtering Works

To appreciate how filtering software works, you first need to understand a little about data navigation along the "Information Super Highway." Data travels along the Internet in the form of electrical signals that form "packets" of information. If you send an email to someone, your mail is disassembled, or "chopped up," into packets that get sent along the Internet and arrive at the recipient's "Email Post Office." The computer that receives the email reassembles the packets to form your message. A similar process happens when you participate in a chat room or make reservations online.

Accessing web pages follows this same disassembly / reassembly process. On the Internet, web site addresses are made up of "IP Addresses," which is basically a defined set of numbers such as 143.5.22.7. When you type an address such as www.internetproductivity.com into your web browser, a "DNS server" resolves that "www name" or URL (Uniform Resource

Locator) into an IP address such as 125.22.33.44, which is what the Internet recognizes and uses to get your information where it needs to be.

In computer networking, devices such as routers, firewalls, proxy servers, and other devices can "filter" information packets based on the address the packets are traveling to and from. For instance, if your employees are visiting a site called www.naughty-pictures.com, then you can tell your filtering software to block all traffic to and from that site. You can also block traffic to and from www.waste-time-at-work.com, www.get-a-new-job-today.com, www.cause-a-sexual-harassment-lawsuit.com, www.get-them-sued-for-copyright-violation.com, and www.gamble-your-life-away.com.

Some filtering software will even read the packets to search for offending words and phrases, such as "sex," "hot babes," "on-line trading,"



“games,” and so on. You can also filter based on the type of traffic attempting to travel. For example, you may decide to allow regular web pages to load but filter out photographs, movies and video, music and audio, and programs that could potentially contain computer viruses.

Many companies who use Internet filtering software believe it is the answer to encourage employee productivity and discourage abusive surfing. Unfortunately, Internet filtering software may not be the answer they’ve been looking for. While it does restrict their employees’ Internet usage, filtering software may actually be causing more harm than good.

The Downside to Internet Filtering Software

The biggest downfall to Internet filtering software is the unspoken message it sends to employees. When employees know their Internet usage is limited, the immediate conclusion is that the company doesn’t trust them. Without that sense of trust, there’s little hope for employee loyalty. This can lead to high turnover levels and increased security issues when it comes to the company’s proprietary information. Ultimately, filtering software gives your employees the impression that “big brother” is watching every move, making your employees less likely to enjoy their jobs and give the extra effort that can lead to greater company profits.

Additionally, because filtering software only blocks the sites you specifically indicate, it can soon become a huge administrative task to update that list constantly. With new web sites launching every day, it’s nearly impossible to block every objectionable web site. Those companies who are committed to making the filtering software as updated as possible often must hire administrative staff solely for this purpose or must pay an outside company to administer and update the filtering software’s blocked list of sites. Both these options can cost companies a considerable amount of money.

Even more unfortunate is that filtering software can sometimes lead to greater levels of Internet misuse. Once employees learn they can’t access certain sites, those with some technical expertise may view the filtering software as a game or puzzle that needs to be cracked. As a result, they spend an inordinate amount of time online, trying to “break through” the software’s barriers and gain

access to the forbidden sites. Those who do manage to beat the system not only waste precious work hours and the company’s revenues, but they also share their new accomplishment with co-workers, which undermines the entire goal and investment into the software.

Filtering Alternatives

Because of the potential drawbacks filtering software presents, many companies have chosen to forego this technology in lieu of some simpler yet equally effective options. These options include, but are not limited to, implementing a strong Internet Usage Policy, educating employees about how to be productive and effective with the time they do spend on the Internet, and promoting the employees’ realization of how harmful Internet misuse can be to their own well-being, both in their personal and professional lives. These solutions will be discussed further in future articles.

End the Misuse Today

As the Internet continues to pervade all aspects of business, its impact on the workplace will steadily increase. The more that employees abuse their at-work Internet connection, the more that technological tools, like filtering software, will come into existence. But before you invest your company’s profits into a tool that promises to end Internet misuse, consider the solution’s overall impact on your company’s bottom line, morale and culture. Sometimes the simpler and less expensive options are your best alternatives.

About the Author:

Mike Foster's history as the CEO of a computer company for 12 years, and as an international technology consultant and speaker, makes him an expert at both technology and management skills. Mike Foster is a frequent presenter of keynote speeches, seminars, and workshops. His message about how to use technology to increase profits and productivity is welcomed by small business owners and Fortune 10 executives alike. For more information about Foster's programs, call 800-657-7107 or visit www.fosterinstitute.com or www.internetmisuse.com.