READY NET GO ... NEWS

September 2004   http://www.readynetgo.net   **610-856-0990**

Tip of the Month

Using the History Feature in IE to Find a Web Page That You Visited

Have you ever stumbled on an interesting Web page, wanted to return to it, but forgot where it was?

Internet Explorer 6 automatically records Web pages you've visited both today and in the past. It organizes them in folders on the History bar by the day you visited.

To find pages in the History list:

1. On the Internet Explorer (IE) toolbar, click the History button (It looks like a green arrow pointing down – if you look really close you'll see a clock face too). IE opens the History bar on the left side of the screen.

2. In the History bar, click the time period you want to search. Click the Web site folder to open the list of pages, and then click the link to the page to display the Web page itself.

3. When you've finished using the History bar, click the Close button (X in the upper right corner of the sidebar).

Note: You can specify how long IE will keep web pages in History. Go to Tools, then Internet Options. Verify you are on the General tab. In the History section type in the number of days you want web pages stored. A typical range for storing web pages is 14 – 30 days.

Using the Web at Work

Over the last several years more and more companies have migrated to the Internet for E-Commerce, communications, and the transfer of computer files. It is common practice for each employee to have a high speed internet connection at their desktop. Unfortunately, this has been a mixed blessing for employers.

Employees can access reference materials from around the world and they can quickly communicate with clients, management and co-workers using E-mail. However, employees can also use corporate Internet accounts inappropriately to view pornography, communicate with competitors and conduct personal business. Employees can also unknowingly create security breaches when they download virus infected programs and files from the Internet. For these reasons, it is important for companies to establish and enforce an acceptable use policy for using the Internet.

There are many reasons that an employee's personal use of the company's internet connection can cause problems. Among them:

Lost productivity - As the Internet provides access to a wealth of information and content on almost any subject imaginable, there is significant temptation for personal use by staff. Numerous surveys tell us that a significant portion of work time is lost to personal use of the Internet.

WWW (Websites Worth Watching)

1. www.suessville.com – Official site of Dr. Suess and all his quirky characters

2. www.noaa.gov – National Oceanic and Atmospheric Association – get the latest on the weather around the world. Great pictures of storms …

3. www.itsecurity.com/dictionary/dictionary.htm - Definitions and explanations of common and not-so-common technology words/phrases

Legal liability - Employers have a legal obligation to protect staff in the workplace from content of a racist or offensive nature. If Internet Use Policies are not in place, employees who are offended by another employee's use of the Internet may file grievances or possibly take legal action. Additionally, the downloading of files via the Internet (e.g. software, data, music, pictures, video etc.) whether intentionally or unintentionally, may infringe on property rights of third parties, exposing the organization to possible legal action.

Damage to IT systems and electronic files - The introduction of a virus to an individual PC or corporate network has the potential to cause enormous havoc, leaving a trail of destruction in its wake. If not sufficiently protected, documents may be destroyed and significant time and money may be required to recover PCs damaged in the virus attack.

Increased IT network traffic - Personal use of the Internet may result in staff downloading web pages or large files (e.g. software, data, music, pictures, video etc.) which take up unnecessary network bandwidth. On smaller networks, this can have a damaging effect on business related network traffic.

What can you do?

   There are several software and hardware solutions available which can be implemented to prevent employees from using the internet inappropriately. If these solutions are not cost effective, there are other ways of monitoring company internet use. Call our office if you'd like to learn more about any of these options. Regardless if you use a technological solution or not, all companies should create a written policy and inform all staff members.

Develop Policy

   In an effort to prevent Internet abuse, companies should have a comprehensive policy in place. It is a good idea to have each employee sign the policy (people tend to read what they are required to sign). The policy should explain what the company feels is acceptable use of the Internet and it should be clear in defining all internet related systems (including but not limited to: computer equipment; software and operating systems; network accounts providing electronic mail, World Wide Web browsing; File Transfer Protocol) which are owned by the company to be used for business purposes. It should also explain that the data created on these systems remain the property of the company and the systems will be monitored. You can find several examples of "Acceptable Use Policies" for Corporate Internet Systems by doing an internet search, keywords "acceptable use policies and internet". *Make sure to run the policy by your legal counsel before implementing.*

Implement the Policy

   Having a policy and not enforcing it is like having speed limits but not giving tickets to those who speed. If you find that someone has broken company policy, be prepared to follow through with reprimands. Also remember to review the policy periodically as staff members change or as you become informed about new hardware/software solutions. All staff members should be encouraged to use the internet as a source of information. Setting up internet use policies will not only help guide your staff so that they can be most efficient in their tasks; it will also help keep your systems running efficiently.

Thanks to Linda for contributing to this month's newsletter