Controlling Internet Misuse At Work

Surfing non work-related sites during working hours reduces productivity, wastes resources, and there can be legal repercussions if inappropriate material ends up on servers or desktops. We explain what you can do to combat these hazards.

By Debbie Wilde
Freelance Writer

An April 2001 survey from Websense (see box) compared Internet misuse in the UK, France, Germany and Italy. It found that the average amount of time spent surfing non work-related sites was three hours and six minutes per week - more than 35 minutes per working day. A similar survey from US-based vault.com found that 47% of employees admitted to spending between 10 minutes and an hour each day surfing non work-related sites, and 24% spent more than an hour a day.

Whereas no-one doubts the huge gains in efficiency Internet access and email can bring for many workers, such facilities can also be a huge distraction for undisciplined or underemployed users. When misuse is widespread, productivity can fall and it can dramatically affect the company's bottom line. According to the Websense survey, 89% of respondents thought the Net could become addictive for some people, and surely we've all noticed how time can fly past when online.

Vault found that a surprisingly high 66% don't believe Internet misuse at work decreases productivity, and Websense found that only 29% of respondents minded their co-workers accessing non work-related sites during work hours; both suggest a widespread culture of complacence among employees. Only 31% would consider either reporting or personally reprimanding co-workers who misused the Internet (Websense).

Bandwidth

Obviously some types of Internet use are more bandwidth-hungry than others. Downloading music files or large graphics, streaming video and online games-playing are all major culprits, whereas the occasional brief email isn't going to make much difference to your bandwidth amongst the legitimate traffic. If you've been having bandwidth problems and you're considering increasing provision, you might first want to consider how much difference it could make if your company cracked down on misuse. A new AUP (Acceptable Use Policy), employee education, and perhaps monitoring or additional filtering capabilities, and you might not need that extra bandwidth after all.

Legal Liabilities

While specific laws and liabilities will vary from country to country, there are two main ways in which your company can become vulnerable as a result of Internet misuse. Firstly, if users download illegal material (such as prohibited pornography) onto your company servers, ignorance of its presence is often not a defence, and the directors of the company may be legally liable (check your local law). Secondly, employees can sue the company for sexual harassment or a "hostile workplace environment" if they are constantly exposed to or targeted with inappropriate and offensive material in the office. Vault found that more than 50% of respondents had received sexually explicit or otherwise improper emails, with 13% claiming to have received such emails frequently. Not only can such incidents be extremely costly, worse still can be the damage to the company's reputation if the story gets out, and that may take a long time to repair.

Your company probably already has an email disclaimer message attached to the bottom of every outgoing email. Ensure this says what it needs to say, since use of a disclaimer can reduce the company's legal liability if employees send inappropriate emails. Secondly, your company will be partially protected from legal liability for employees' abusive actions if you have in place an Acceptable Use Policy which states clearly what the company considers acceptable and unacceptable.

Acceptable Use Policy

Your first line of attack for reducing Internet misuse in your company should be to implement or overhaul your AUP. You should have one of these anyway, but if it's become buried and seldom referred to then it's time to update it, check it says what it needs to say and then bring it to the attention of your employees. Websense's survey found that only 41% of UK employees believed their employer had an Internet AUP, with France, Germany and Italy tailing at 16%, 27% and 17% respectively.

It's worth viewing the updating of the AUP as an opportunity to educate your employees about the risks and downsides to misusing the Internet at work. Instead of treating them like small children, try to involve them in the process so they buy into it and understand how it can benefit everyone. No likely software solution can exert complete control, so you want to foster an atmosphere of trust rather than the reverse. For instance, you need to consider whether you will ban employees from using the Internet for personal use altogether (this may be considered draconian and thus ignored), or whether you will instead impose limits and time restrictions on personal use. With the long working hours often expected these days it may be more realistic to permit some limited use, since users have less and less time outside the work environment to perform simple functions such as checking a bank balance or booking some tickets.

Surveillance And Morale

Research from the American Management Association in 2001 shows that 77% of major US firms record and review employee activities at work, such as phone calls, email, Internet connections and computer files, and this figure has doubled since the AMA first asked these questions in 1997. Figures vary for each monitoring activity, but nearly 63% of companies surveyed in 2001 monitored Internet connections, and 46% stored and reviewed email messages. Vault.com found that 53% of employees believed their employer monitored their Internet / email usage, whereas only 41% of employer respondents claimed they did.

If you plan to monitor what your employees are doing at work you need to take into consideration their feelings. Alienating the entire workforce does not lead to higher productivity, and higher productivity is one of our goals. Websense found that 71% of employees felt it was acceptable for their employer to manage Internet access at work, either by written policy, filtering software, monitoring software or managers walking around, but these four methods were considered acceptable in descending order at 74%, 65%, 41% and 20% respectively. Vault found that only 53% of employees felt comfortable with their email and Internet use being monitored.

Employees have come to regard email in particular as their private space, even when sent / received with company resources on company time. It's viewed by most as a private conversation, in the same way as a private chat by the coffee machine or a quick phone call to a mate to arrange to meet. Moves for IT or other staff to routinely read employee email are likely to cause considerable friction, and thus the issue needs handling with care. The dissatisfaction which can come from draconian rules and monitoring can be counter-productive. Internet misuse, rather than simply a technology problem, can be viewed as a management and morale issue: happy employees who feel valued, and who have plenty of work to do, are less likely to grossly misuse company resources.

Discipline

However, if your AUP states that certain actions will be taken against those who violate the rules, it's important that these threats are realised, else the rules won't be taken seriously. So make sure you don't threaten actions you would be unwilling to carry through.

The American Management Association found that 18% and 20% of companies surveyed had dismissed employees for misuse of email and the Internet respec-

Favourite Forms Of Misuse

According to the Vault survey, the most popular non-work Internet function accessed by employees from their work desks was reading the news (72%), followed by travel arrangements (45%), purchases (40%), job search (36%), hobbies, stock checks and planning social events. Downloading music came in at 13% and playing games at 10% - both high-bandwidth pursuits. Pornography, frequently portrayed as the main evil of the Web, accounted for only 4% of work-time Internet misuse according to the survey of employees.

The European-based survey from Websense recorded the most popular categories as travel (51%), educational (42%), hobbies (41%), shopping (28%) and sports (27%).

Dedicated Content Filtering Solutions

Websense Enterprise is a dedicated Internet access management software solution. See also **www.websense.com/products/about/competitors/index.cfm** for Websense's competitive comparison with similar products from other vendors.
www.websense.com

SurfControl SuperScout Web Filter and Email Filter.
www.surfcontrol.com

Elron Internet Manager Web Inspector
www.elronsw.com/productfamily/webinspector.shtml

Secure Computing SmartFilter
www.securecomputing.com/index.cfm?skey=85

SonicWALL Content Filtering
www.sonicwall.com/content-filter/solutions.html

Content filtering for small business and educational establishments.
www.cybersitter.com/cybinfo.htm

tively, at least 38% had issued formal reprimands for email / Internet misuse and at least 24% informal reprimands. According to Vault, 80% of employers reported having caught an employee surfing non work-related sites at work, but the survey does not cite action taken. Websense found that an average of only 13% of respondents across the UK, France, Germany and Italy knew someone in their company who had been disciplined for Internet misuse at work, with the UK figure considerably higher at 26%.

Practical Measures: Monitoring And Filtering

Filtering and monitoring software can increase your control of the situation, enforce your AUP, and is best used in conjunction with the "softer" methods outlined above rather than instead of. The concept began with "net nanny" software aimed at home users wishing to protect their children, but is now being utilised to protect companies from the actions of their adult employees. Internet access management software comes in a number of different guises:

Gateways

Much content filtering comes as part of an integrated package of security software which sits at the company's Internet gateway and also provides facilities such as intrusion detection and anti-virus protection. This type of software can require the onsite administrators to manually select which URLs and keywords to disallow, and thus the amount of control is limited by the time the administrators can spend on updating the lists.

Lists

Some content filtering vendors also provide "control lists" or "blacklists" - lists of sites which are disallowed. Lists of prohibited sites usually include pornography, weapons, hate, subversive and drug-related sites, and sometimes also gambling, sport, news, shopping and entertainment sites. "Overblocking" can sometimes occur when the control lists are produced automatically by Web "crawlers", which search for trigger keywords and for graphics with certain ratios of skin-tones, because these processes are not foolproof (corporate photographs often contain a high proportion of skin-tones, for instance). Control lists need to be up to date, since many of the sites you'll want to block frequently change their URLs; sometimes a subscription is payable to the vendor for the latest lists.

White Lists

Alternatively, "whitelists" can be used, which instead of blocking the specified sites only permit the specified sites. This means you can just permit sites relevant to your users' work needs, and don't need to update the list so regularly. However, the

Misuse: The Dangers

- Loss of productivity.
- Loss of available network bandwidth.
- Violating copyright laws by downloading / uploading copyrighted files.
- Sending sexual, defamatory or hate mail.
- Downloading pornographic or obscene files onto company servers.
- Creating a "hostile work environment" by use of inappropriate email or files.
- Lawsuits against the company for permitting sexual harassment or a "hostile work environment".
- Bad publicity for the company following legal action or dismissals for misuse.
- Employees intentionally passing on sensitive company information to outsiders.

downside is that it can be too restrictive, and is not really suitable for users who may need to use the Web for legitimate work-related research.

Sniffing

Some content filtering software does not use control lists but instead "sniffs" the contents of files as they're being downloaded. If the file is found to contain inappropriate triggers then various actions may be taken, such as blocking the file or logging the abuse.

Quarantine

If email is subject to control then content detected as potentially unacceptable may be quarantined until a manager can view it and take action. Bear in mind that such policing of mail can become onerous, and will cause great employee resentment if innocent emails are delayed for long periods.

EIM

A few companies provide what Websense calls Employee Internet Management software - an integrated package designed specifically for filtering, monitoring, reporting and managing employee Internet use. This type of package can track your employees' usage, telling you which sites they are visiting and how much time they spend online. Some software can even take screenshots of online activities, showing you exactly what your users are looking at.

Websense

To give a flavour of what is available, we will briefly look at one of the market leaders in the dedicated Internet access management market, Websense Enterprise (**www.websense.com/products/index.cfm**). The main application is a server-based software solution which can be run on a variety of platforms (Windows 2000 or NT, Sun Solaris or Red Hat Linux) and permits you to set policies. This comes with the Websense Master Database, which consists of 500 million pages of Web content classified into more than 75 categories. Websense Reporter completes the package.

Websense uses pass-through filtering by integrating with a firewall, proxy server or caching device (such as CheckPoint FireWall-1 or Microsoft Proxy Server). Each request is checked against the Master Database and then logged for reporting purposes. You can configure the application to block, permit, time-limit or postpone access to each category by user, group, workstation or network. The Database is updated daily and can be automatically downloaded, and Websense WebCatcher helps you optimize it for your specific needs. Websense Reporter allows you to evaluate how your users are using their Internet access.

Conclusion

If you suspect that some of your users are misusing workplace Internet facilities in any way which could endanger the profits or reputation of the company, it's worth taking action now to assess and curtail the problem. The only way to be certain of the extent of the abuse may be to install monitoring software, but before such a purchase you may wish to make a preliminary investigation based on the evidence available - anecdotal experience from supervisors, and any logs your current software may provide.

Assess the extent of the problem, identify the key risks to your company and decide on an appropriate solution, which may be a combination of employee education, updating and promoting your Internet AUP, and upgraded filtering, monitoring and reporting software.

PCNA

The Surveys

www.vault.com/surveys/internetuse2000/index2000.jsp

www.websense.com

www.amanet.org/research/summ.htm

www.surfcontrol.com

Copyright ITP, 2001

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.

Tech Support Alert
http://www.techsupportalert.com