

## **Solving Business Threats Caused by Improper Use of the Internet by Employees**

*A recent study by Salary.com and America Online found that U.S. employees squander an average of two hours of company time online every day, time that costs their companies \$759 billion annually.*

## Summary

Employees spend many hours on the Internet, and much of the time isn't used for their work. A recent study by Salary.com and America Online found that U.S. employees squander an average of two hours of company time online every day, time that costs their companies \$759 billion annually.

Employers face serious problems with employees' improper use of the Internet, including:

- Unauthorized access to websites that charge a fee to enter
- Sexual harassment charges by employees due to the display of pornographic or obscene materials on adult websites
- Trademark and copyright-infringement issues from improper use of materials owned by an outside party
- Viruses from downloads of software and other materials found online
- Lost productivity because company time is wasted by employees surfing the Web for non-work-related activities

## Potential Consequences of Internet Misuse

### Malicious Content

Often, material downloaded from or viewed on the Internet raises security concerns. Contact with a compromised website can bring destructive viruses into the company's network and cause significant damage.

Also, in today's world, employees are constantly downloading a variety of applications — including those for instant messaging, peer-to-peer file sharing, voice-over Internet protocol (VOIP) and proxies — that can be easily installed without the approval of a company's IT group. Such applications pose the risk of being infected with viruses that will then be transmitted onto the organization's network. Often, those viruses cause illegal and malicious e-mail spam to be disseminated from the company's computers.

Spam now accounts for around half of e-mail sent globally and is becoming a major headache for companies. Around 65% of spam is sent on hijacked computers, using insecure software already installed on employees' machines.

### The Risk of Liability

A significant area of potential liability is improper end-user online behavior that involves use of the company domain name. For example, most organization domain names identify the company name and when the user communicates via the internet the company brand is at risk.

For example, if employees log onto Internet chat rooms or send e-mail messages that contain the company domain, improper statements made by the employee may be attributed to the company. This can lead to claims of defamation, discrimination and unfair competition simply because someone happens to see — and possibly print a hard copy of — the improper statements.

Another area of potential liability involves improper use of company computers to access the Internet. An example of this would be if an employment claim or lawsuit is filed against an organization, it is standard procedure for a plaintiff's lawyers to inspect computer records. Since deleting a user's computer files doesn't completely erase them—many traces are left on the computer — forensic computer experts can easily find incriminating data and use it against a company. If inappropriate activity took place and is discovered, the entire organization can be at risk.

## Offensive Material

It is common knowledge that offensive conversations in an office setting can result in legal ramifications for organizations. Similarly, employees being exposed to sexually explicit or otherwise offensive material on a colleague's computer screen, can create an uneasy — or even contentious — working environment.

Leading organizations have not been immune to this problem. In 2000, *The New York Times* fired 22 employees in Virginia for allegedly passing around potentially offensive electronic mail. The same year, Xerox fired 40 workers for spending work time surfing pornographic and shopping sites on the Web.

Dow Chemical Company fired 50 employees in 2000 and suspended another 200 for up to four weeks without pay after an e-mail investigation uncovered hard-core pornography and violent subject matter. The violations were made by workers at all levels in the company; Dow's investigation was sparked by an employee complaint.

As part of an ongoing corporate crackdown in 2000, employees and contractors at pharmaceutical giant Merck & Company faced discipline — including dismissal — for inappropriate e-mail and Internet usage.

The following statistics illustrate the significant amount of improper Internet usage by corporate employees:

- An IDC Research/Harris interactive poll reports that the average employee spends more than 8.3 hours per week on non-work-related Internet use.
- A Computer Crime and Security survey reported that of the 503 companies it surveyed, 78 percent detected employee abuse of Internet access privileges (e.g., downloading pornography or pirated software, or inappropriate use of e-mail systems).

These results should be alarming to any company that is concerned with their brand or reputation because such a high degree of misuse of the Internet can severely damage an organization's image as well as its profitability.

## What Organizations Need to Know

### One Approach: Establish Internet Use Policy

At a minimum, every company that provides Internet access for its employees should have a detailed Acceptable Use Policy (AUP) in place. Similar to other company policies, the AUP should clearly define:

- Where employees can and cannot go online
- When they can surf the Internet for personal reasons
- Which types of online activity is strictly forbidden
- What consequences will result if the policy is violated

Employers should be realistic and flexible when developing an AUP, recognizing that some personal Internet use may be appropriate. Also, employers should make sure their staff understands not only the rules, but also the rationale behind the AUP. Employees are more likely to adhere to a policy when they recognize and appreciate its necessity.

### Web Blocking Vs. Web Monitoring

A 2005 survey of 526 organizations by the ePolicy Institute and the American Management Association found that 76 percent of the companies surveyed monitor the websites that their employees visit and 65 percent block certain sites. At least 55 percent of the organizations review and retain employees' e-mail, and 36 percent track the content on workers' PCs, their keystrokes and the time they spend at the keyboard.

***Spam now accounts for around half of e-mail sent globally and is becoming a major headache for companies. Around 65% of spam is sent on hijacked computers, using insecure software already installed on employees' machines.***



These are important controls for company Internet activity:

- Establish acceptable sites for browsing
- Block pop-ups and Web advertisements, which are typically infected with adware
- Establish time periods when personal Internet surfing can take place
- Scan files for viruses

Blocking software takes an active approach to preventing Internet abuse by employees. By blocking objectionable sites on company computers, companies can stop employees from creating potentially dangerous situations. This is most easily accomplished by installing Internet blocking software on the company computers to control Web access.

Web-blocking software prevents employees from visiting websites that the company deems harmful or offensive. Web-monitoring software, on the other hand, lets the employer monitor employees' Internet use without barring access to websites.

Software makers have developed employee website monitoring programs that can be installed on employee machines remotely from a central location. Website monitoring packages provide many useful capabilities: restricting employee access to certain internet sites, preventing installation of other software, logging employee activity and application usage (including video capture of screen activity and even logging every key pressed by the employee during computer operation).

The blocking versus monitoring question is the source of much debate. Monitoring software doesn't bar employees from visiting undesirable sites, but productivity tends to improve when employees know they're being monitored. Employees usually can't make an argument when an employer confronts them with evidence of their Internet abuse.

If the employer does not wish to actually restrict employee Internet browsing, monitoring lets them keep a record of which sites the employee goes to. Often, the knowledge that the employer can monitor Internet use is enough to discourage employees from improper use of the company Internet access.

Organizations don't necessarily have to choose between monitoring and blocking. Often, the best solution is to combine the two methods by blocking sites that clearly violate corporate policy and monitoring other Internet usage.

### **Software Vs. Hardware**

Another key issue is whether to adopt a software-only or hardware-based system. Software-only applications can be complicated to manage and often require their own server.

Hardware appliances are simpler to implement — many of them can block certain sites or categories right out of the box and centralize website management. But appliances are often much more expensive than software-only solutions, which can be too expensive for small-to-midsize businesses.

There is another option: A managed service for Web security and control that reroutes Internet traffic through a Managed Security Service Provider (MSSP). David Mitchell, group product manager of security service vendor MessageLabs, describes this solution: "If a company uses a software- or appliance-based solution, they might have to obtain new appliances, other hardware, licenses, backup procedures, hot standby machines, networking checks or load balancing. On the other hand, if the company uses a managed service, no additional hardware or software is needed and updates or changes in policy settings are managed by the MSSP."

### **One Complete Solution**

A comprehensive answer to the problem of inappropriate Internet use is MessageLabs Web Security Services. The solution incorporates a powerful range of multi-layered technologies that ensure total protection from external and internal web threats.

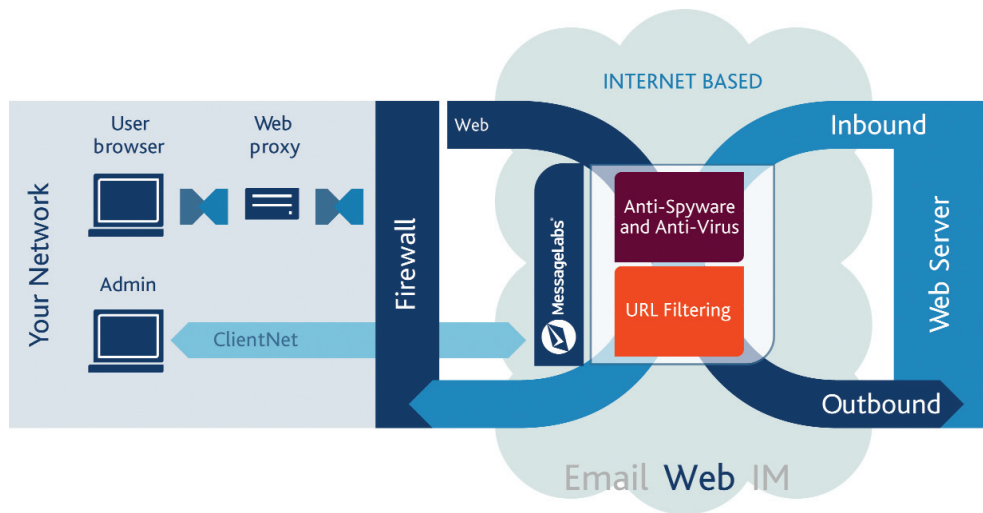
Using data from its analysis of threats, the proprietary Skeptic™ technology detects new and converging malware. Best-of-breed commercial scanning engines provide impenetrable defenses against known viruses and spyware. A URL categorization database in MessageLabs Web Security

*In 2000, The New York Times fired 22 employees in Virginia for allegedly passing around potentially offensive electronic mail. The same year, Xerox fired 40 workers for spending work time surfing pornographic and shopping sites on the Web.*

Services controls web use in compliance with your acceptable-use policy and blocks access to websites known to distribute spyware.

Combining multilayered malware protection and industry-leading URL filtering capability, MessageLabs Web Security Services provides direct business benefits that enhance everything a company does.

The diagram below illustrates the managed-service aspect of the MessageLabs Web Security Services solution.



***A 2005 survey of 526 organizations by the ePolicy Institute and the American Management Association found that 76 percent of the companies surveyed monitor the websites that their employees visit and 65 percent block certain sites.***

With MessageLabs Web Security Services:

- All web traffic requests pass through the MessageLabs platform, hosted in secure data centers worldwide
- Each request is checked against a company's acceptable-use policy, determining whether it is blocked or allowed to pass
- Different rules can be applied to different user groups and individuals
- If a request is allowed to pass, the relevant web page or file download is scanned for malware by Skeptic™ and multiple, continually updated third-party technologies
- ClientNet, a customized extranet, tailors your online experience to your organization's needs
- If a malware threat is identified, access to the web page is denied

MessageLabs Web Security Services provides protection from external malware threats and internal web misuse by combining industry-leading technology with efficient service and customer support. MessageLabs Web Security Services is fully scalable and provides:

- 100 percent service availability supported by a robust global infrastructure
- Total protection, via Skeptic™, from emerging threats targeting web users
- Quick and easy set up with predictable and affordable total cost of ownership
- 24/7 support in an extensive range of languages, worldwide
- Unsurpassable Service Level Agreements (SLAs) that will assure availability, reliability, and most importantly effectiveness of MessageLabs services. The SLAs also provide clients a clear definition of the exact service levels they can expect to receive when working with MessageLabs.

To learn more about MessageLabs Web Security Services, visit [www.messagelabs.com](http://www.messagelabs.com).





**Americas**  
**AMERICAS HEADQUARTERS**

512 Seventh Avenue  
6th Floor  
New York, NY 10018  
USA  
T +1 646 519 8100  
F +1 646 452 6570

**CENTRAL REGION**  
7760 France Avenue South  
Suite 1100  
Bloomington, MN 55435  
USA  
T +1 952 830 1000  
F +1 952 831 8118

**Asia Pacific**  
**HONG KONG**  
1601  
Tower II  
89 Queensway  
Admiralty  
Hong Kong  
T +852 2111 3650  
F +852 2111 9061

**AUSTRALIA**  
Level 2  
107 Mount Street  
North Sydney  
NSW 2060  
Australia  
T +61 2 8208 7100  
F +61 2 9954 9500

**SINGAPORE**  
Level 14  
Prudential Tower  
30 Cecil Street  
Singapore 049712  
T +65 6232 2855  
F +65 6232 2300

**Europe**  
**HEADQUARTERS**  
1270 Lansdowne Court  
Gloucester Business Park  
Gloucester, GL3 4AB  
United Kingdom  
T +44 (0) 1452 627 627  
F +44 (0) 1452 627 628

**LONDON**  
3rd Floor  
1 Great Portland Street  
London, W1W 8PZ  
United Kingdom  
T +44 (0) 207 291 1960  
F +44 (0) 207 291 1937

**NETHERLANDS**  
Teleport Towers  
Kingsfordweg 151  
1043 GR  
Amsterdam  
Netherlands  
T +31 (0) 20 491 9600  
F +31 (0) 20 491 7354

**BELGIUM / LUXEMBOURG**  
Culliganlaan 1B  
B-1831 Diegem  
Belgium  
T +32 (0) 2 403 12 61  
F +32 (0) 2 403 12 12

**DACH**  
FeringasträÙe 9  
85774 Unterföhring  
Munich  
Germany  
T +49 (0) 89 189 43 990  
F +49 (0) 89 189 43 999

[www.messagelabs.com](http://www.messagelabs.com)  
[info@messagelabs.com](mailto:info@messagelabs.com)

© MessageLabs 2007