



Employee Web Use and Misuse: Companies, their employees and the Internet

A MessageLabs Whitepaper; October 08

MessageLabs Web Security service gives companies the ability to monitor and enforce their internet usage policies.

Internet Use and Misuse

Where do you draw the line? Is it okay to send the occasional personal email at work? What about a little internet shopping or spending sometime on social networking sites, playing online games, downloading pirated movies and music, gambling or downloading porn? The internet has created new opportunities for mischief and new challenges for managers.

Worldwide worries

In today's office environment, employers have a relatively new issue to deal with; employees wasting time online and putting your business at risk. A large proportion of corporate web traffic is non-work related: gambling, music downloads, personal webmail, social networking and even pornography sites.

According to The ePolicy Institute, of the 30% of bosses who terminated employees for web violations in 2007, 84% cited the viewing, downloading or uploading of pornography and otherwise offensive or inappropriate material as the reason.¹

Unwanted websites

MessageLabs protects thousands of businesses from inappropriate web use. Blocked sites fall into the following categories:

Categories	Most Blocked Sites
Advertisements & popups	44.5%
Chat	28.3%
Streaming media	4.7%
Unclassified	4.0%
Games	3.2%
Downloads	2.0%
Personals and dating	1.9%
Adult/sexually explicit	1.8%
Web-based email	1.7%
Blogs and forums	1.2%

Source: MessageLabs Intelligence, July 2008

Web misuse can have serious implications for your business:

- **Reduced productivity.** If employees spend their time on a social networking sites such as Facebook, they're not spending it doing their job.
- **Security problems.** Malware hides on websites and can install itself as users browse infected pages. MessageLabs Intelligence reports that the number of new, malicious websites blocked each day by MessageLabs nearly doubled (91 percent) in just one month with 3,968 new sites intercepted daily.²
- **Legal risks.** When users download inappropriate material to their computers other employees may take serious offense which in turn can create legal liabilities for managers.
- **Wasted bandwidth.** Internet connections cost money. If half your bandwidth is taken up with non-work related web traffic, you could potentially be paying twice as much as you need to and your business-critical communications could be running at half their speed capacity.
- **Unlicensed software.** When users download and install software from the internet, they create a legal risk. Software piracy is illegal. If an organization uses illegal copies of software, it may face a civil suit and company directors risk criminal penalties.
- **Reputation risk.** Social networking can create opportunities for employees to leak confidential information or spread damaging rumors online. Bad behavior by a single employee can reflect on the reputation of the whole organization.

Blocking non-business internet access

In the face of all these problems, many managers' first reaction might be to block all employee access to the internet.

It makes sense to block certain sites outright. Pornography sites are an obvious example, but most companies may also consider gambling and game sites as utterly unrelated to work, potentially time-wasting and block them as well. Ninety-six percent of employers who block web access are concerned about employees visiting adult sites with sexual content. Companies also use URL blocks to stop users from visiting game sites (61%), social networking sites (50%), entertainment sites (27%) ; sports sites (21%) and external blogs (18%) according to the 2007 Electronic Monitoring & Surveillance Survey from American Management Association and The ePolicy Institute.³

¹ Not Just Words: Enforce Your Email and Web Acceptable Usage Policies ; Author Nancy Flynn, Director, The ePolicy Institute

² MessageLabs Intelligence Report July 2008: www.MessageLabs.com/resources/mlireports

³ 2007 Electronic Monitoring and Surveillance Survey from American Management Association and The ePolicy Institute. Survey results available at www.epolicyinstitute.com

However, completely blocking internet access may not be the right approach for your business.

Monitoring employee behavior online

Monitoring inappropriate use may seem to be the lesser of two evils compared with blocking access to large parts of the internet. Having blocked the worst websites, you may wish to trust your employees' judgement. You may want to allow employees access to social networking sites if it means that they can organize their social life without spending hours on the phone. You might also allow people to shop online if it saves them time and lets them achieve a better work-life balance.

Keep in mind, when you decide to allow employees access to the internet, it is in your best interest to ensure that they are aware of the laws around electronic communications in the workplace. The federal Electronic Communications Privacy Act (ECPA) makes it clear that a company-provided computer system is the property of the employer. U.S. employers have the legal right to monitor all employee computer activity, transmissions and content- including incoming, outgoing and internal email messages, as well as web surfing, downloads and uploads. Making sure your employees are aware of the laws surrounding internet usage may encourage them to use better judgement when surfing the net.

Policy matters

It's clear that blocking or monitoring web use requires careful thought. Any decision needs to be backed up by a clear, acceptable usage policy for the internet. The MessageLabs sponsored whitepaper, *Not Just Words: Enforce Your Email and Web Acceptable Usage Policies (AUP)*, written by The ePolicy Institute, is a good resource to help determine what should be covered in your AUP.

Each company has its own ethos. Some managers may take a more laissez-faire approach while others want to lock everything down. Some people need full access to the web and companies may wish to give some departments or individuals more latitude than others. A good example is your Human Resources department who might use Facebook or LinkedIn for recruiting purposes. The use of social networking sites may be suitable in that capacity, but your Finance department may not have a work-related use for such sites.

When thinking about employee internet access and your company's well-being, consider the following:

- **Do I have a solution in place that can effectively block web-born malware, viruses and spyware?**
- **Does my solution allow me to create web filtering and monitoring rules for different groups or employees? How flexible is my solution?**
- **Have I clearly defined a written Web Acceptable Usage Policy?**

In the end, it comes down to choice. Where do you draw the line? How do you balance individual access with the overall protection and good of the business? What is the correct balance between monitoring and blocking? There is no right answer. It varies from company to company. But there is, perhaps, a right way to go about it.

Our Solution: MessageLabs Web Security Service

Because the MessageLabs service operates in the company's network of data centers, there is no hardware to buy, no hefty up-front capital costs, no ongoing upgrades or maintenance and no software licences; just a predictable per-user fee.

From a single portal, managers can set up policies – blocking sites individually or by category. They can also set different policies for different types of users. The same ClientNet portal gives managers detailed reports on internet use in their company. In addition to policy management, Skeptic™ technology gives MessageLabs a unique – and powerful – way to protect its clients against web-born malware. When your employees ask for a web page, the request goes through our system first so we can scan the page for malware and check it against your company policies.

The MessageLabs Web Security service gives companies the ability to monitor and enforce their internet usage policies; whether they are very restrictive or very liberal, whether they favor monitoring or blocking. MessageLabs service brings site monitoring and URL filtering together with industry leading anti-virus and anti-spyware protection. As the world wide web becomes an increasingly more important business tool, companies need the best possible solution to help protect their computer systems, their reputation and their employees. MessageLabs delivers those tools.

For more information or to sign up for a FREE Trial, please visit www.message-labs.com/trials/free_web.

MessageLabs service brings site monitoring and URL filtering together with industry leading anti-virus and anti-spyware protection.

⁴ Not Just Words: Enforce Your Email and Web Acceptable Usage Policies ; Author Nancy Flynn, Director, The ePolicy Institute



www.messagelabs.com
usinfo@messagelabs.com
TOLL FREE 866-460-0000

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 14
90 Arthur Street
North Sydney
NSW 2060
Australia
T +61 2 9409 4360
F +61 2 9955 5458

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
40 Whitfield St
London W1T 2RH
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
usinfo@messagelabs.com

© MessageLabs 2008

©2008 MessageLabs Inc. All Rights Reserved. MessageLabs and the MessageLabs logo are registered trademarks and Be certain is a trademark of MessageLabs Ltd. and its affiliates in the United States and/or other countries. Other products, brands, registered trademarks and trademarks are property of their respective owners/companies. WP_WEBUSE_1008

WHITEPAPER: **Employee Internet Use and Misuse** : Companies, their employees and the Internet