

## IN THIS ISSUE

AUGUST 2003

*Spam in the Workplace Raises Significant Issues for Employers Both in Terms of Lost Employee Productivity and Potential Liability From Failing to Protect Employees From Receiving Offensive Spam.*

## OFFENSIVE SPAM IN THE WORKPLACE: EMPLOYERS' OBLIGATIONS AND LIABILITIES

*By Jennifer J. Walt, Patrick H. Hicks, and Wendy Medura Krincek*

---

### DEALING WITH SPAM IN THE WORKPLACE

---

Since the mid-1990's email has become as essential to the workplace as telephones and facsimile machines. However, the increase in usage of email has led to a very troubling by-product – an enormous increase in the sending of unsolicited commercial emails, known as “spam”, from opportunistic and often unethical individuals. Spam has been increasing dramatically worldwide and is causing significant business disruption at all levels. It is estimated that spam has risen from 8% of all email sent in 2001, up to 40% of all emails currently sent and is expected to reach 50% by the end of the year. Various studies have shown that spam is having a detrimental effect on worker productivity, network utilization, mail storage systems and employee morale. Therefore, it is important for employers to both familiarize themselves with this problem and with ways to deal with the growing tide of spam.

---

### THE PROBLEM

---

Employers have dual concerns regarding spam in the workplace: liability and productivity. On the liability front, employers could potentially face liability for their failure to sufficiently protect against and respond to offensive spam that reaches employees. Many employees must utilize email as part of the day-to-day duties of their job. Unfortunately, this means that employees must wade through spam, sometimes of a pornographic nature. Courts have already found that the proliferation of pornographic images in the

workplace can create a hostile environment for employees. Fresh territory waiting to be explored includes whether an employer's failure to implement or update appropriate safeguards to limit pornographic spam could also create a hostile work environment, even though such emails are sent by third parties having nothing to do with your business. An additional area of potential liability for employers is whether employers are appropriately responding once they become aware of offensive spam in the workplace, including disseminating to employees a reporting procedure whereby employees can apprise the employer of their receipt of offensive emails.

On the productivity issue, having employees wade through unsolicited emails containing pornographic images and commercial advertisements is certainly not the way most employers want employees to spend their work time. Time spent wading through and dealing with spam by employees is lost revenue to employers. Spam is also a source of technical problems, sometimes overloading servers to the point of crashing them which, again, results in lost time and money to your organization. Additionally, spam is sometimes used to spread worms and viruses that cause havoc to computer networks and can destroy data.

---

### WHY IS SPAM SPREADING SO RAPIDLY?

---

Since spam first began proliferating, software companies and internet service providers have been hard at work developing spam-blocking software

meant to identify and dispose of spam before it ever makes it to an email account. However, spammers have been working equally as hard at coming up with creative ways to get around spam blocking software. The end result is that spam-blocking software installed just a year or two ago is not sophisticated enough to block current spamming techniques. For example, spammers now create messages that look like they are coming from internal email address within an organization. Additionally, spammers are using images instead of words since spam-blocking software is meant to catch and dispose of emails containing certain key words, not visual images. In addition, spammers are also embedding non-viewable codes and symbols between the letters of key words that spam-blocking software is often set up to catch thereby evading those filters.

---

#### WHAT IS BEING DONE ABOUT SPAM?

---

For the past several years Congressional legislation has been proposed to make spamming a federal offense. This year is no different. At least five different bills have been introduced in Congress aimed at restricting unsolicited commercial email. This year's proposed legislation ranges from creating a national "No-Spam Registry" whereby email users could register their email address and choose not to receive unsolicited commercial email; to making it a criminal offense to relay multiple commercial electronic mail messages that mislead recipients as to the origin of the email; to creating an "opt-out" list whereby email users would have to individually notify each sender of spam that they did not want to receive such emails.

In addition to efforts being made to curtail spam at the federal level, several states including Washington, the home of Microsoft, have already passed anti-spam

legislation. Such laws are making it possible for internet service providers and software companies such as Microsoft to take the lead in attempting to stem the rise in spam by bringing private lawsuits. Microsoft recently filed 15 lawsuits in the United States and United Kingdom against companies and individuals allegedly responsible for billions of spam message sent in violation of state law. These suits were filed against alleged spammers who try to fool email recipients by providing false information in the "from" line of an email or using deceptive subject lines, such as "your loan application." However, these efforts are unlikely to have any effect in the immediate future.

---

#### WHAT YOUR ORGANIZATION CAN DO

---

Most employees have and need access to email. It is virtually impossible to eliminate all spam from the workplace, but there are several steps employers should take to minimize the impact of spam on the workplace both in terms of productivity and potential liability.

- Implement or revise email policies to instruct employees to bring inappropriate, especially sexually inappropriate emails, to the company's inattention.
- Reevaluate whether it is time to update anti-spam software. The technology in this area is constantly changing as spammers figure out how to avoid being caught in the net of anti-spam software from years past. Thus, employers should periodically evaluate whether current software is effectively eliminating spam in the workplace.
- Educate employees on your anti-spam software. Such software is equipped with settings whereby users can have emails containing certain

key words or phrases automatically deleted while adding the sender's name to a junk email list preventing future emails from that sender from being put through. However, such features are useless if your employees do not know how to use them.

- Educate employees on how to respond to spam. Even with the most effective anti-spam software available, some spam will inevitably make it through to your employees. Often people are tempted to take unsolicited email senders up on their offer to reply and request to be removed from the mailing list thinking this will prevent them from receiving future emails. To the contrary, responding to spam simply informs the spammer that they reached a real email address and, better yet, that the email user actually read their email! Thus, responding to pornographic or other offensive spam by requesting to be removed or to unsubscribe from the mailing list often has the opposite effect and results in even more spam being sent to the user.
- Instruct employees and set up policies only permitting use of the internet when it is work-related. If some non-work related internet use by employees is permitted, advise employees to stay away from chat rooms, forums, and discussion groups.

Using these steps and staying abreast of current advances in spam blocking software should assist employers in limiting potential liability and lost productivity.

---

*Jennifer J. Walt is associate general counsel in Littler Mendelson's San Francisco office, and Patrick H. Hicks is a shareholder and Wendy Medura Krincek is an associate in Littler Mendelson's Las Vegas office. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, Ms. Walt at jwalt@littler.com, Mr. Hicks at phicks@littler.com, or Ms. Krincek at wkrincek@littler.com.*

---



