Winter 2003/04—Vol. 6, No. 1

Small Business CANADA MAGAZINE

"Written to Help!"

Cash Management

Getting the most out of your hard-earned money!

PLUS:

- Review of Microsoft Office Small Business Edition 2003
- Test your telephone effectiveness
- Stop whining and start leading!
- A guide to reducing spam
- ...and so much more!

$3.95 CDN – WINTER 2003/4

WWW.SMALLBUSINESSCANADA.CA

A guide to *reducing* spam

by Tristan Goguen

Unsolicited e-mails that advertise everything from university degrees to porn is filling up e-mail inboxes. Commonly known as spam, these e-mails are more than a nuisance. It costs money and time to deal with. According to IDC's report "Worldwide E-mail Usage Forecast, 2002-2006", spam accounts for approximately 30 per cent of all traffic flowing through the Internet.

Spam mail can be damaging to your business in many different ways. Some spam mail contains viruses, which can attack key critical business files or computer systems. Others try to trick you and your employees into installing keystroke capture programs (perhaps disguised as an "unsubscribe" link) that allow a hacker to remotely monitor everything you type.

Most people delete spam as soon as they see it in the inbox. But have you ever considered how much time is spent each week cleaning out the inbox? Each employee will have wasted 15 hours deleting e-mail in 2003 compared to 2.2 hours in 2000 according to a Ferris Research report "Spam Control: Problems and Opportunities". This will cost the average business $400 per in-box in lost productivity in 2003.

Tips on minimizing spam

The best way to avoid spam is to not be on a spam list. Here are ideas to make it harder for spammers to find your business e-mail address.

Do not post a text hyperlink to your e-mail address on your Web site. Post it as a GIF or JPEG image. Customers can read the address, but automated Web crawlers that explore Web sites to compile e-mail lists will not detect it.

On your Web site, use a form field that does not display your e-mail address, but allows a Web site visitor to submit a message. Another option is to dedicate one e-mail address for Web site communications so only this address is revealed. You will keep your personal addresses from being exposed. Incoming mail to your public address can be viewed separately from your main business e-mail.

Use public and private e-mail addresses. Use generic, free e-mails such as Hotmail or Yahoo for contest submissions, online registrations, or posting to discussion groups. You can abandon that address when spam becomes uncontrollable. Give your private address only to legitimate contacts.

Never reply to spam, not even to unsubscribe. Doing so indicates your e-mail address is valid.

E-mail programs with a preview capability (such as Outlook's preview pane) should be turned off. You are actually "opening" the mail when it is previewed. This can tip off the spammer that your address works. There is also a chance a virus can be activated if you preview an e-mail.

A wide variety of anti-spam solutions

There are varieties of software and service solutions available to reduce spam. Depending on how your business uses e-mail, some solutions will fit better than others. Here are a few common anti-spam technologies used today.

White List Technology—A pre-authorized address book maintained by the user. New e-mail contacts that arrive are flagged for your review, requiring permission to be added to your list. Another variation is once the sender sends an e-mail to you, the sender receives a message with an instruction to click a button to verify he or she is not an automated mass-e-mailing program. Once on your list, e-mail exchanges flow naturally.

Black List Technology—A collection of illegitimate e-mail addresses, domain addresses and IP addresses is created. E-mails originating from these listed sources are blocked. Spammers are constantly falsifying their sending location so this technology may not be effective at blocking the newest spam messages. Legitimate e-mails can accidentally be blocked, including e-mails originating from entire countries with high spam rates.

Content/Category Filters—These filters use rules to process the e-mail. It scans incoming e-mail for tip-off terms and words, unlikely return addresses, unusual symbols, embedded graphics, and fraudulent routing information. The filter calculates the violations and ranks the e-mail to determine if it receives a passing score, in which case it will arrive at your inbox. A failing score sends an e-mail to a quarantine folder.

Key things to look for in an anti-spam solution

Compatibility—Some anti-spam solutions are not compatible with all e-mail programs. Check carefully for one that works with the variety of e-mail programs being used in your office.

Quarantine Area—This folder stores spam so you can occasionally review to ensure your legitimate e-mails did not get blocked. A medical/health-related professional may find this feature important as words commonly filtered pertain to names of drugs.

Effectiveness—Anti-spam solutions do not all work the same. An effective anti-spam solution will block almost all your spam with the exception of a few. An effective solution will not block any legitimate e-mails.

Seamless Processing—Does the anti-spam solution allow you to retrieve your e-mail in the same manner as you did before the installation? A good anti-spam solution should not require you to perform extra steps to protect your e-mail.

Ease of Use—Is the product easy to install? Is it easy to use? SBCM

Tristan Goguen is President of Internet Light and Power Inc., one of North America's premier Internet Service Providers. Tristan is proactively helping businesses and individuals find ways to reduce spam. Contact Tristan at tgoguen@ilap.com for more information on his efforts or visit his Web site.

WWW.ILAP.COM