

The True Cost of Spam

Spam, junk mail, unsolicited electronic messages – whatever you call it, it's a nuisance and a royal pain in the inbox. But it is more than an inconvenience – it can be costing your business thousands, if not millions, of dollars each year.

There are a number of different ways to quantify the true cost of spam. There is the lost productivity, time being distracted from daily work either reading spam or trying to get your IT team to get rid of it. And then there is the downtime caused by crashed computers or servers attacked by viruses or trojans. When you look at the figures, it's startling what costs you could be avoiding if only you could figure out how to stop the dreaded spam.

A little aside here about the origin of spam....

The term 'spam' came to be used to refer to the large scale or repetitive delivery of something unwanted after a Monty Python skit about the tinned luncheon meat.

1937: Hormel Foods in Minnesota introduces its "new miracle meat in a can; tastes fine, saves time".

1970: The Monty Python's Flying Circus "Spam" skit is televised.

1978: The first spam email is sent (ironically, by a marketer at a computer company, so you be the judge as to who the real culprit is).

2007: The 7th billionth can of Spam is sold.

2007: The NZ Department of Internal Affairs introduces the Unsolicited Electronic Messages Act 2007.

2009: Current reports estimate that 90 to 95% of emails being sent are spam.

It's more than just a nuisance – it's hurting our economy

The amount of spam reaching our inboxes and the cost to businesses are serious concerns. According to the NZ Department of Internal Affairs, "the negative effects of spam are significant and far-reaching. Current estimates suggest that around 120 billion spam messages are sent every day. These emails clog up the Internet, disrupt email delivery, reduce business productivity, raise Internet access fees, irritate recipients and erode people's confidence in using email." (source: *The Department of Internal Affairs* <http://www.antispam.govt.nz>)

Given that between 90 and 95% of all email traffic is spam (according to both the *Cisco Annual Security Report 2008* and *Symantec's MessageLabs Intelligence Report May 2009*), these 'negative effects of spam' are costing New Zealand businesses billions in a number of ways:

1. Lost productivity

There is a great deal of time and expense associated with lost productivity. Spending just 10 minutes a day dealing with spam will cost you almost a full week of lost productivity every year. Multiply that by the number of employees in your business and soon it's the equivalent of shutting shop for a month or two each year.

2. Wasted IT resources

As a frequent source of viruses and trojans, spam is tremendously wasteful of your IT resources, using up your disk space, backup space and bandwidth. Even if users delete spam emails, unless they are deleted from all folders, they may end up remaining stored in archive folders and on server back-up drives.

For government departments, law firms and any other business that is required to save communications for a certain length of time, having to store a copy of all emails received can be largely impacted by spam making its way to user desktops. The key is to stop these emails before they even get into your system, so that spam is never stored or archived.

3. Identity fraud

It goes without saying that most 'offers' marketed by way of spam are fraudulent. Responding to them greatly increases your risk of suffering identity theft. Many spam emails are phishing schemes, scams asking you to provide some of your personal details – name, email address, password, bank details – all so that the senders can impersonate you for fraudulent purposes.

4. Rising ISP costs

Because of the online obstructions and email delivery disruptions that spam causes, it adds significantly to your ISP's costs - costs that they inevitably pass on to you, the customer.

5. Problems for mobile users

The problem for a lot of computer users, particularly people who are away from their desk a lot and retrieve their emails on the road, is that spam is not blocked at the server level and it makes its way to an individual's BlackBerry, iPhone, smartphone or PDA. The impact could be extremely costly to your business. Most mobile packages charge for incoming messages whether they be a call, SMS or email, either on a per-message rate or per KB of data received. In reality, then, you are paying for every spam message that makes its way to your hand-held device, whether you open it or not. Here, too, you run the risk of reaching your data cap if your monthly plan has one.

So what can you do to combat spam?

Despite all of the associated risks and costs to the business, a lot of small and medium enterprises (SMEs) have come to tolerate a certain amount of spam, frustrated that they can't seem to do anything about it. It's put in the 'too hard' basket because it is a never-ending nuisance; something left to the IT guys to sort out.

Just what are your options as a business owner? Do you have to concede to a certain amount of spam, or can you do more about it?

There are two main ways to try to combat spam. The first is through the use of the many software spam filters currently available. A software spam filter is software that you can either purchase as a separate program or that comes with your email system. The software looks for certain words in the body text and subject line of an email message, as well as reviewing the actual email address of a sender to determine whether an email is suspect or not. Most businesses already have some sort of spam filter running on their computers and a lot of spam is stopped this way. However, spammers are getting more sophisticated and are figuring out how to out-smart these filters, so large numbers of spam emails are still making their way through. If you rely on this type of filter, software must be purchased and installed for each user's PC and you've got to stay current with new releases and upgrades to the software.

To further realise why filter software is not enough, you only need a rudimentary understanding of how they work. Spam filters look at emails once they've come into your network, and filter them before they get distributed to the individuals they are addressed to. Think of the filter as sitting in the reception area of your business. They've opened the front door, and then they work on determining whether the entrant is a welcome visitor or an intruder before allowing them up the lift. However, in the case of spam, already this is too far in.

By the time a spam email enters your organisation (allowed into the reception area by the filter), it is already costing you money. Even if the email goes no further, never making it to the inbox of the intended recipient, it is already using up your organisation's bandwidth and data storage. You also run the risk of viruses and trojans making their way onto your company server.

Another way to try to reduce the amount of spam coming in to your business is by using an anti-spam appliance (also called an email security appliance). The appliance is a piece of

hardware that sits on your network alongside your email server. Appliances are becoming more popular and, for several reasons, seem to be better able to deal with the problem of spam – primarily because they block spam *before* it hits your email server (unlike filtering software that only filters emails once they're in).

How the costs add up

The risks and costs associated with spam are greater than most non-IT people realise. They agree that spam is a nuisance for them (and their one inbox), but they aren't fully aware of how big the aggregate problem is for a company.

In 2007 information technology research and advisory firm Nucleus Research estimated that spam costs employers US\$712 per employee annually through loss of productivity (a figure arrived at by calculating the number of spam emails survey respondents were receiving, time estimated handling spam messages, work hours per year and average wage levels).

We looked at a typical New Zealand SME, a company with 12 desktop computers and 10 mobile devices. On average, they received 8000 emails per day, with 90% being spam. Of these, 80% were being stopped by the company's server based filtering software (7200 spam emails received; 5760 stopped; 1440 spam messages getting through every day). In one month, then, 43,200 emails allowed through to the individual users' email clients were spam. The costs and consequences were:

- 2 hours per month per employee spent sifting through spam for legitimate emails
- 40 emails received containing malicious attachments or links
- 2 malicious attachments or links actually opened
- 1 hour per month spent in contact with the outsourced IT company to deal with spam or spam related issues
- approximately 2340 MB of storage space on their server used by unwanted emails
- roughly 420 MB per user per month of mobile data used to forward unwanted incoming spam that wasn't blocked before making its way to the company's smartphones

To put a (conservative) figure on it, these expenses cost the company somewhere around \$18,000 to \$20,000 per year. It's the equivalent of at least \$1500 per employee annually. And this of course excludes the unknown lost opportunity costs that arise from genuine emails being lost in the clutter, or mistakenly deleted along with the spam. For a larger company, these costs multiply.

So don't underestimate what you may have simply thought was just a nuisance and a bit of a time waster. Spam is not just a technology issue. If you are a business owner or manager, ask your IT manager to show you the figures. And then invest the money in an effective email security appliance.

Then, to cheer yourself up, go out and hire the Monty Python's DVD megaset.

David White is owner and managing director Digital Kiwi Ltd, who are the producers of Spam Gate™.

Spam Gate™ is a state-of-the-art email filtering system that is guaranteed to prevent 99% of unsolicited commercial email. For more information, contact info@spamgate.co.nz or call 0508 48 48 48.

www.spamgate.co.nz

www.digitalkiwi.co.nz