

Spam emails

July 2007

Why's it called "Spam"?

A famous Monty Python sketch revolved around a restaurant, which specialised in dishes with the meat product, "Spam".

A group of Vikings sat in the corner were singing "Spam, Spam, Spam, lovely Spam, wonderful Spam!" - drowning out all the conversations in the restaurant.....

Like the Vikings' singing, email "spam" can drown out the useful emails you do want to receive.

Our E-Business Advisers discuss ways of avoiding this nuisance:

1. What is spam?

One definition of spam is an "unsolicited email message, usually sent in bulk and commercial or promotional in nature".

Most spam messages are commercial advertisements for products or services, which may include 'get rich quick' schemes, pornographic material, hoax messages, jokes and chain letters.

Use of email is critical for just about every business today, enhancing our ability to communicate quickly and easily.

As email has become an important marketing tool for legitimate businesses, unscrupulous 'junk emailers' or 'spammers' have picked upon

this opportunity to use this easy and inexpensive channel to sell their wares to millions of potential customers across the world.

2. Everyday examples of spam

- Prescription Drugs & "Body enhancements"!
- Get rich quick schemes
- Low rate mortgages
- Software to spy on your friends
- Instantly clear adverse credit history
- Special offers

3. Too much spam isn't good for you!

What makes spam such a big problem is the ever-increasing amount of it.

Spammers try all the tricks, including every possible permutation of email addresses to see which ones are valid

Despite all the latest developments in anti-spam technology, unsolicited messages continue to arrive in our email in-boxes at an alarming rate.

Business email servers are flooded with spam messages and Internet Service Providers (ISPs) have to cope with steadily increasing traffic.



Fact Sheet

- Spam "attacks" disrupt electronic messages and transactions, filling up your company's email boxes.
- Unsolicited messages require additional system resources for processing and storage
- Staff regularly waste otherwise productive time dealing with spam
- Staff can be annoyed or offended by spam, resulting in legal problems for employers
- Legitimate marketers' reputations suffer because of the proliferation of unsolicited commercial advertisements
- Anti-spam legislation is difficult to enforce

4. Where is all this spam coming from?

Spammers can be individuals or organisations, who 'harvest' email addresses from web sites, mailing lists and newsgroups.

There is also a brisk trade in email address lists amongst the spammer community - and some spam emails offer to sell you these lists!

They send their messages out in bulk to just about anyone they can find – generally to thousands of people who have never expressed any prior interest in their products or associated services.

Some spam messages contain fraudulent or illegal offers, relying on the lack of knowledge of its recipients.

Email message headers can often be forged or tampered with to conceal their identity and location, and recipients who click on a spammer's "remove me from this mailing list"

link are often only confirming that they have a live email address - thus inviting more spam!

Never click on the unsubscribe link on a spam email.

Unsolicited text messages received on mobile phones are also classed as spam. Don't reply - just delete these too.

Offensive or pornographic messages can also threaten business Internet policies, often inviting the unwitting recipient to open a message which may potentially violate internal Internet usage policies.

5. Protecting your business from spam

Unfortunately, there is no 100% effective way of protecting your company email in-boxes from spam.

However, there are lots of ways that you can significantly reduce the amount received or the potential risks to your staff.

One aim should be to make sure your computer systems are secure, as many computer viruses spread themselves using spam.

- Educate your staff by helping them understand the risks
- Enforce company email policies
- Install anti-spam software
- Install anti-virus software
- Update virus definitions regularly
- Install Firewall protection



Fact Sheet

There are a wide range of anti-spam software applications on the market today, of which two of the most popular are McAfee's SpamKiller and Norton AntiSpam.

Both software packages include a number of powerful tools which can be set up to allow messages from a 'white' list of email addresses, and block messages from a 'black' list of spammers already plaguing your email in-boxes.

Your anti-spam software is unable to 'guess' the address of every email you receive in advance, so you can also create lists of 'white' and 'black' words to help identify spam.

For example, you might want to block messages containing the word "Viagra" - unless you're a pharmaceutical company!

Unfortunately, the way around this is simple for the spammers - they would use V i a g r a (with extra spaces between the letters). This is still totally readable for a human, but unlikely to be picked up by anti-spam software.

Anti-spam software has often been developed to 'learn' over time, to identify more accurately what is and isn't spam based on the type of messages you simply delete or choose to open.

In the same way as there is a constant war between computer virus writers and anti-virus companies, spammers and anti-spam firms are involved in an ongoing battle too.

6. Spam and the law

From the 11 December 2003, a new European Directive, the 'Privacy & Electronic Communications Regulation' now makes it illegal to send unsolicited emails. Recipients

now have to "**opt-in**" to receive marketing emails.

There are exceptions for mail messages sent to business addresses, for further information please refer to the Useful Links section below.

1st New Rule

This rule applies to all marketing messages sent by electronic mail, regardless of who the recipient is.

- The sender must not conceal their identity **AND**
- The sender must provide a valid address for opt-out requests

2nd New Rule

This rule only applies to **unsolicited** marketing messages sent by electronic mail to **individual subscribers**.

Senders cannot send such messages unless they have the recipient's prior consent to do so.

The strict "opt-in" rule is relaxed if 3 exemption criteria are satisfied:

- The recipient's email address was collected "in the course of a sale or negotiations for a sale"
- The sender only sends promotional messages relating to their "similar products and services" **AND**
- When the address was collected, the recipient was given the opportunity to opt out (free of charge except for the cost of transmission) which they didn't take



Fact Sheet

- Also, the opportunity to opt out must be given with every subsequent message.

However, the problem is that most spammers are outside of the European Union (many are based in the USA or Russia) - and refuse to take note of the European legislation.

Whilst they are almost impossible to track down and prosecute effectively, the daily flooding of our email boxes continues!

7. Useful Links

www.ico.gov.uk - Information Commissioners web site, with details about the "Privacy & Electronic Communications Regulation"

www.websitezone.com/directory/Integrate-Advanced-Tools/Networking-Tools-Utilities/Spam-Filter
Web site with useful links to Anti-spam products

And finally -

<http://www.detritus.org/spam/skit.html> - A little "light relief" - the text of the Monty Python sketch!

Disclaimer: we have no commercial links with these companies or their products, and their appearance in this fact sheet is not an endorsement