Managing Spam

Expert knowledge means success

Contents

Note: This publication has not been updated since it was last published. Some of the hyperlinks may have changed and may need updating. In addition, some of the information in this publication may be out of date.

Introduction

Spam is electronic junk mail, but it can be more offensive and cause more damage than the paper variety. Brightmail - a spam protection software provider - estimates that 50% of all e-mails sent are spam. Billions of spam e-mails are stopped each day from reaching customer's e-mail inboxes by ISPs and e-mail software.

This publication will help you understand what spam is, how it tries to get to your inbox, and what measures you can employ to stop it.

Sending spam is a profitable business: advertisers can use it to reach an audience of millions with minimal delay and minimal cost. Any response, however small, can generate a profit.

Typical spam subjects include:

- debt reduction;
- purchasable qualifications;
- gambling;
- body enhancement; and
- pornography.

Spam may not cause obvious or catastrophic damage to your computer system, but it can still harm your business and other businesses in the following ways:

- spam, particularly in the form of chain letters, can clog up network traffic;
- spam can be offensive, both in the subject line and in the content and companies have a duty to protect their employees from such material;
- spam can be sent from another innocent business whose computer system has been hijacked;
- managing spam – without spam protection software – can be time consuming; and
- where it is difficult to differentiate between spam and legitimate e-mail, the legitimate e-mail may be deleted, or the spam may be read.

Tricks of the spammer's trade

As more computer users have become smarter about Spam and how to deal with it, so the advertisers have found more creative ways of getting Spam into your inbox. The following are typical devices used:

- subject lines may appear as business e-mails to lull you into a false sense of security;
- subject lines may have common spam keywords altered to try and fool spam filters while leaving the subject matter still discernible by the reader;
- common spam keywords may be disguised in HTML codes – there are numerous ways this can be done including using the numeric equivalent of a letter, using spaces of size zero between the letters of a keyword, or making words invisible by setting the background colour to equal the font colour;
- common spam keywords can be split into HTML tables which when concatenated form the keyword; and
- spam may be sent "from" your address to an invalid address so that it is returned to you as the "sender".

If the Spam protection software determines that the e-mail is likely to be spam it will block it from reaching your inbox, or delete it depending on your selected settings.

Spam and Viruses

Spammers do not want to be traced. If a spammer can "take over" a computer system, by means of a virus, it can then use that machine to send out its spam and decrease its own traceability. It is estimated that more than 30% of spam is now sent by this method (Source: Sophos). Collusion between spammers and virus writers works both ways: a virus writer can spread their virus quickly and efficiently is they use a spammer's address list.

Government launches IT security alert service

On 23 February 2005, the UK Government launched IT Safe – a rapid alerting service that tells computer users about serious internet security problems. It aims to provide both home users and small businesses with proven, plain English advice on protecting computers, mobile phones and other devices from malicious attack.

Advice is available on the IT Safe website and through SMS or email alerts. For more information visit: www.itsafe.gov.uk

Tackling Spam

There are a number of measures you can take to reduce the spam you receive. These include taking care of how and where you publish your e-mail address, using the inherent anti-spam facilities of your e-mail software and installing spam protection software.

Guarding your e-mail address

The privacy of your e-mail address will determine the amount of spam you receive. Guard it as you would your home phone number. If a spammer knows your e-mail address is a valid one, not only will he use it, but it could be added to a mailing list sold to other spammers.

Don't publish your e-mail address online: spammers use "web bot" software to pick up published e-mail addresses. If you have a website, use either an "E-mail us" button which directs to an HTML "disguised e-mail address" or a submittable form rather than publish your e-mail address on the site. If you must publish your e-mail address, for example when using a newsgroup or chat room, disguise it. A common method is to use 0 instead of O, so that your address can be interpreted by a reader, but not picked up by a web bot.

Consider using multiple e-mail addresses. In addition to your main address, you could set up an e-mail account specifically for Web transactions and registrations so that any resultant spam is directed to this secondary e-mail address. Your mail e-mail address could then be given solely to friends and colleagues.

Check the privacy policy of any websites whose services you sign up for. Ensure that you don't agree to your e-mail address being released to third parties. If in doubt, opt-out of receiving further information.

Protecting your inbox

Even if you keep your e-mail address private, you can still be vulnerable to spam. Spammers send out e-mails to millions of random e-mail addresses: invalid addresses are returned to the sender, so the spammer can easily determine which addresses are valid.

Guidelines for Reducing Spam

Don't publish your e-mail address
- If you publish your e-mail address online, a spammer can pick it up.

Consider using multiple e-mail addresses
- Give your main e-mail address to friends and colleagues and use an alternative e-mail address for online registrations.

Be wary of automatic subscriptions
- When filling in on-line forms, opt out of receiving further information.

Check the privacy policy of websites
- Don't agree to your e-mail address being released to third parties.

Don't open e-mails from an unknown source
- If you don't know the sender, delete the e-mail. If you open it, it may alert the spammer that your e-mail address is active, or it may activate a virus.

Be wary of opening attachments
- Even if you know the sender, it is best practice to save an attachment, to allow virus checking software to check the attachment on opening.

Don't use the 'preview' mode in your browser
- The preview setting has the same effect as opening your e-mail. Previewing your inbox may inform a spammer that you have received their message.

Don't reply to spam
- If you reply to spam, you indicate that your e-mail address is active. It may then be included in a list sold to spammers. "Unsubscribing" from a dubious mailing list is one example of this.

Use the blind copy field
- Use the BCC field rather than the "To" or "CC" field when e-mailing a number of people simultaneously. This will hide the list of recipients from other users.

Never buy from unsolicited e-mail
- Do not trust your money to advertisers who market their goods and services in this way.

Take advantage of anti-spam features provided by your e-mail software
- Use built in spam filters and configurable security settings to reduce the spam you receive. If available, configure your e-mail software to block images, as these can be used to inform a spammer that your e-mail address is valid.

Install and use Spam protection software
- Spam protection software can reduce your unsolicited e-mail and delete it or filter it out of your inbox.

One of the most effective ways to protect your inbox is to delete all unopened e-mail if you don't know the sender. If you open the e-mail, it may alert the spammer that your e-mail address is active, or worse still, it may

Victory against Spam

A ground breaking victory has opened the way for businesses that suffer from large numbers of spam emails to bring damages claims against the spamming companies.

In December 2005, a businessman, Nigel Robert, used recent European laws (that allow recipients of unwanted commercial emails to claim damages) to sue Media Logistics UK for damages in respect of the junk emails sent to his personal e-mail account.

Media Logistics did not defend the charge and settled out of court for £270 damages plus the cost of filing the claim.

While not significant in amount, it could be significant in principle, and it is hoped that the settlement acts as a deterrent for spamming companies.

But beware - this result also means that your business should be extremely wary of sending unsolicited emails to existing/past customers. If you receive any indication that they may not want to receive your emails then don't send them.

activate a virus. If your browser has a "preview" facility – don't use it! The preview setting has the same effect as opening your e-mail. Previewing your inbox may therefore inform a spammer that your e-mail address is active. Take special care with attachments. Even if you know the sender, it is best practice to save an attachment, to allow virus checking software to check the attachment on opening. Alternatively, you could send an instant message to the sender to request confirmation that they are the genuine sender.

If you reply to a spam e-mail, you alert the spammer that your e-mail address is active. It may then be included in a list sold to other spammers. "Unsubscribing" from a dubious mailing list is one example of this.

If you receive an apparently legitimate e-mail from a company you trust, in which you are asked for personal information, check that the e-mail is legitimate before providing the information. Telephone the company using a contact phone number you know is correct, rather than the number in the e-mail.

Avoid participating in chain e-mail messages. Chain e-mail can be used by spammers to gather active e-mail addresses. Once you join the chain, you have lost control of where your e-mail address will go. If you need to send a legitimate e-mail to a large number of recipients, use the blind copy field "BCC" rather than the "To" or "CC" field. This will hide the list of recipients from other users and help protect their addresses.

Never buy from unsolicited e-mail: you will be trusting your e-mail address, and any personal or financial information provided to the advertisers who market their goods and services in this way.

Using the anti-spam features in your e-mail software

Take advantage of anti-spam features provided by your e-mail software and ISP
Your e-mail software may have built in spam filters and configurable security settings to allow you to reduce the spam you receive. Any spam received can be filtered into a separate inbox so you can review e-mails received by the spam inbox and check whether an e-mail is spam, and can therefore be deleted, or is a legitimate e-mail which can be read.

Configure your e-mail software to block images, as these can be used to inform a spammer that your e-mail address is active. Some e-mail software packages are preset to automatically block images from people who are not in your address book.

Your e-mail software may also offer other protective features. For example Microsoft®[1] Outlook®[2] includes the following anti-spam features:

- a configurable protection level, which is set by default to "Low" – sufficient to detect obvious spam. This level can be set to "High";
- an updatable junk e-mail filter; and
- an adult content filter.

MSN®[3] Hotmail®[4] includes the following anti-spam features:

- an intelligent spam filter that can determine particular instances of spam and filter them into a separate inbox for review;
- an option to delete spam before it arrives in your inbox (us this option only once you are sure that only spam e-mails are being identified as such);
- the possibility to create a virtually spam free e-mail account using a combination of the "Contacts" list, "Safe" list and the "Exclusive" filter setting;
- automatic initial blocking of images sent by anyone not on your "Contacts" list;
- an option to automatically report spam and block the sender;
- automatic virus scanning of e-mail attachments;
- verification that accounts are registered to real people; and
- a restriction on the number of e-mails one account can send each day.

If you have an e-mail server, for example Microsoft® Exchange, you can configure anti-spam features at the server end before they reach your e-mail client software.

Using spam protection software

Spam protection or "Anti-spam" software can detect unsolicited e-mails and filter them to a separate inbox or delete them before they reach your inbox. Typical features include:

- looking for keywords that frequently appear in spam e-mails;
- looking for alterations to keywords that suggest an attempt to fool a spam filter;
- looking for unwarranted HTML code which could be harbouring a message;

UK businesses are ignoring "spam laws"

A report by data management firm CDMS indicates that a third of the 200 UK cross sector top companies they examined are not complying with the European Union's (EU) regulations on unsolicited emails.

Instead of opting into a mailing list, consumers are having to explicitly opt out when signing up for promotional offers or ordering products and services online. As a result they may be illegally added to a mailing list and sent emails that they have not requested.

The Information Commissioner's Office has the power to fine transgressors up to £5,000. UK registered companies usually stop sending emails once they have been contacted and warned by the ICO, but companies that send spam emails from outside the UK are harder to track down.

The ICO has been in talks with the Department of Trade and Industry over what can be done "to strengthen our enforcement powers to deal with the irresponsible minority". Enforcement test cases are expected in the future.

- checking the validity of the originating domain name or web address; and
- blocking of e-mail that comes from a blacklisted address.

Spam protection software should be regularly updated to ensure that it has the details of the latest scams.

There's plenty of anti-spam software available over the Internet - for example:
Qurb - www.qurb.com/products/qurb-spam.php

Mailwasher - www.mailwasher.net/

AntiSpam - www.anti-spam-software.com/

McAfee - http://uk.mcafee.com/root/product.asp?productid=msk

Clearview - www.clearview.co.uk/

Spam Inspector - www.microsoft.com/security/default.aspx

SpamEater Pro - www.spameater.net/

Net Nanny - www.netnanny.com/products/emailprotect

ChoiceMail One - www.digiportal.com/

You can find a review of several anti-spam products at:
http://spam-filter-review.toptenreviews.com/?ttreng=1&ttrkey=anti+spam+software

Reporting Spam

If it is obvious which ISP the spam e-mail has come through (it may be listed after the @sign), return the spam to the ISP with your complaint. Your ISP may also have a specific address to report spamming to; for example if you are using MSN® Hotmail® you should report spam to abuse@hotmail.com.
If you are not sure where to report the spam to, visit The Network Abuse Clearinghouse at www.abuse.net. It keeps a master database of reporting addresses to help the Internet community to report and control network abuse and abusive users. Its sister site: www.spam.abuse.net provides step by step details of how to complain to the spammer's ISP. It also provides useful articles on blocking spam and protecting your e-mail address.

Instant Messages

Instant Messaging is growing in popularity and is therefore another target for spammers. The same rules apply: never open files or attachments from people you don't know. Even if you know the sender of a file or attachment, you may choose to check its legitimacy by sending an instant message to the person who sent the file asking them to verify that they have sent you a message.

Your messenger software may have anti-spam facilities to protect you further. For example MSN® Messenger will allow you to block unwanted messages and alert you when someone tries to add you to their "Buddy list". It can also make use of anti virus software you have installed to scan all file transfers. MSN® Messenger allows you to block unwanted messages.

Further Information

This guide is for general interest - it is always essential to take advice on specific issues. We believe that the facts are correct as at the date of publication, but there may be certain errors and omissions for which we cannot be responsible.

Publication issued or updated on:
27 January 2012

Ref: 681

References:

[1]Microsoft®, [2] Outlook®, [3] MSN® Messenger, [4] Hotmail® and [5] Windows® are registered trademarks of Microsoft Corporation.