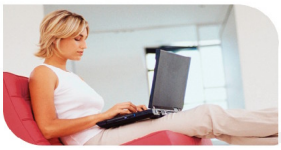
datanet.co.uk
Business Class Internet



White Paper Anti-Spam

DATANET.CO.UK White Paper

Never make a purchase from an unsolicited email.
If spamming weren't economically viable, it would be obsolete. Not only can an email user fall prey to a potentially fraudulent sales scheme, but his or her email address can also be added to the numerous email lists that are sold within the spamming community, further compounding the number of junk emails received.

If you do not know the sender of an unsolicited email message, delete it.
While most spam is usually just annoying text, a spam email message could actually contain a virus and/or other exploit that could damage the computers of all who open it.

Never respond to any spam messages or click on any links in the message.
Replying to any spam message, even to unsubscribe or be removed from the email list only confirms to the spammer that you are a valid recipient and a perfect target for future spamming.

Avoid using the preview functionality of your email client software.
Many spammers use advertising techniques that can track when a message is viewed, even if you don't click on the message or reply. Using the preview functionality essentially opens an email and tells the spammers you are a valid recipient, which can result in even more spam.

When sending email messages to a large number of recipients, always use the blind copy (BCC) field to conceal their email addresses.
Sending an email where all recipients addresses are exposed in the "To" field makes all the email addresses vulnerable to harvesting by a spammer's traps.

Don't provide email addresses on websites.
Many spammers utilise "web bots" that automatically surf the Internet to harvest email addresses from public information and forums. Your web designers can help you in this matter. Email addresses can be encoded using either front end, browser based technologies which robots are unable to decipher, or by using server-side scripting to send emails from a simple online form, without the need to put your actual email addresses on the site.

Don't use your email in newsgroup lists or other online public forums.
A simple technique is to convert the "@" symbol to the word "at", for example: info-AT-datanet-DOT-co-DOT-uk

Never give your primary email address to anyone or any site you don't trust.
Share it only with your close friends and business colleagues.

Have and use one or two secondary email addresses.
If you need to fill out web registration forms or surveys at sites from which you don't want to receive further information, consider using secondary addresses to protect primary email accounts from spam abuse. Also, always look for a check-box that solicits future information/offers, and be sure to select or deselect as appropriate.

Conscientious end users who follow these suggestions will ultimately play a significant role in reducing the amount of spam that enters their organisation's communications system, especially when automated spam-filtering supplements their efforts.