Reference : USER 190
Issue date : January 2004
Revised : November 2007
Classification : Staff
Originator : Richard Rogers

Handling Unsolicited Commercial Email (UCE) or 'spam' using Microsoft Outlook® at Staffordshire University

• •

This document explains how to handle unwanted commercial email that arrives in your email account.

This documents assumes familiarity with both Outlook® and Microsoft Windows® as used on PCs using the staff image at Staffordshire University.

Further useful documentation:

'User191 Setting up Microsoft Outlook® to reject unsolicited email - UCE or Spam, using Microsoft Outlook® at Staffordshire University'
Available in PDF format at:
www.staffs.ac.uk/uniservices/infoservices/documents/userguides/email/

All current Information Services documents for staff and students may be found in pdf format at:www.staffs.ac.uk/uniservices/infoservices/document

What is UCE/spam?

Unsolicited commercial e-mail is the electronic equivalent of the ‘junk mail’ we have all become accustomed to receiving through our letter boxes in recent years. Usually it carries advertising material, ranging from cheap loans, through get-rich-quick schemes to pills and potions, to promotion of pornographic web sites. UCE is popularly called ‘spam’ (thought to be after the Monty Python “spam, spam, spam…” sketch).

Where does UCE come from?

UCE rarely comes from the ‘From’ address shown on the message as seen in the mail client -*Microsoft Outlook*®. These addresses are usually faked to distract attention from the true source of the message. Traditionally, most UCE was sent using - or abusing mail servers that have been incorrectly configured, allowing so-called ‘open relaying’ - meaning anyone, anywhere can use the server to send messages wherever they like.
Recently however, it is more likely to be sent from ‘botnets’, which are PCs infected with viruses that send mail under centralised control.

Why doesn’t the University block these messages?

In short, it is impossible to block UCE completely without also blocking some legitimate mail. Even blocking only messages from open relays carries this risk.

What is the University doing to help me reduce the nuisance?

Information Services has deployed a system using a number of tools including SpamAssassin software, which can help you manage the UCE you receive.

SpamAssassin examines every mail message entering the system and assigns it a score based on the similarity of its content to typical UCE messages. If this score exceeds 5, the message is tagged ‘{Spam?}’ before it is delivered to you.

How can I take advantage of the SpamAssassin system?

Using the *Microsoft Outlook*® Rules facility - (see User 180 *Microsoft Outlook*® at: www.staffs.ac.uk/uniservices/infoservices/documents/userguides/email) you can have the suspected UCE messages moved automatically to a folder where you can quickly look down the list of senders prior to deleting the messages.

The rule would look something like this:

> Apply this rule after the message arriveswith **{Spam?}** in the message header move it to the **Probably Spam** folder and stop processing more rules

Note that although it would be possible to set up a rule to automatically delete messages marked ‘{Spam?}’, we do not recommend this as it is possible that a legitimate e-mail could be tagged in this way.

Some spam isn't tagged – how can I deal with that?

All messages with a SpamAssassin score of 5 or higher are marked '{Spam?}', as mentioned above. However, the actual SpamAssassin score is also inserted into the message header, so if you find this score is too high (so too many UCE messages are untagged) or too low (so too many legitimate messages are tagged – see below), you can use this to set your own preferred threshold. You can do this by setting a rule similar to this:

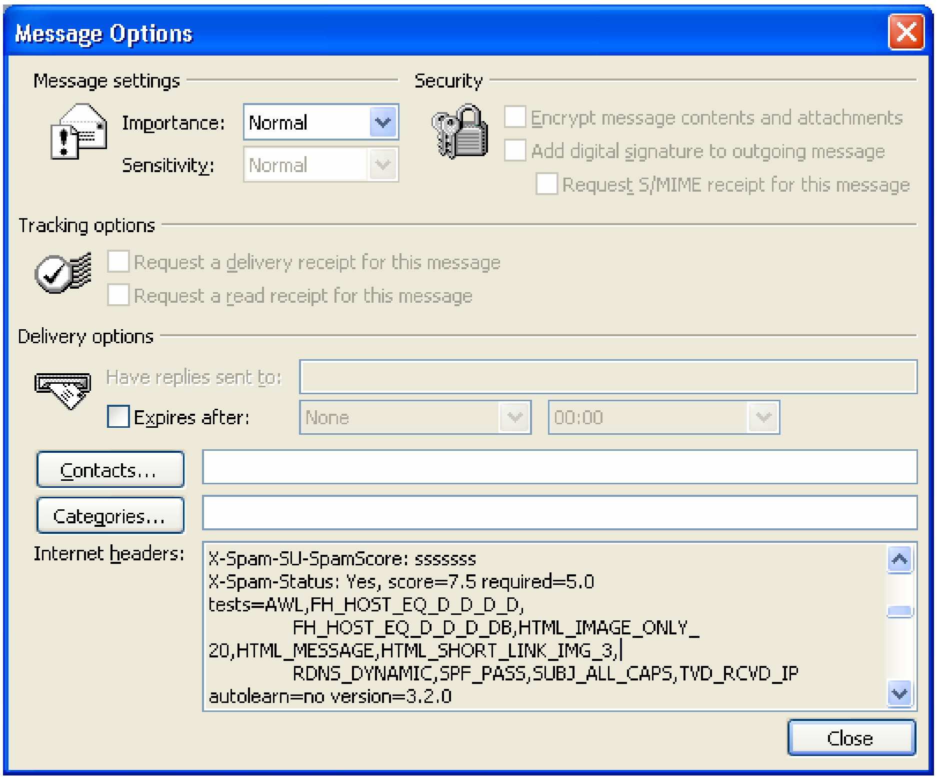
> Apply this rule after the message arrives with
> **X-Spam-SU-SpamScore: sss in the message header**
> move it to the **Probably Spam** folder
> and stop processing more rules

In this case all messages with a score of 3 or higher will be treated as spam. By adjusting the number of s's in the score you can set the threshold to suit your own requirements, remembering that the higher you set the threshold, the more chance there is that spam messages will be left in your Inbox, and the lower you set it, the more chance there is that legitimate messages will be treated as spam.

To view the message headers to look at the scores

Within *Microsoft Outlook*®, right-click an email message and select Options to view the header information.

Browse through the Internet Headers section to see details



Importance: Normal
Sensitivity: Normal

□ Encrypt message contents and attachments
□ Add digital signature to outgoing message
□ Request S/MIME receipt for this message

□ Request a delivery receipt for this message
□ Request a read receipt for this message

Have replies sent to:
□ Expires after: None 00:00

Internet headers:

```
X-Spam-SU-SpamScore: sssssss
X-Spam-Status: Yes, score=7.5 required=5.0
tests=AWL,FH_HOST_EQ_D_D_D_D,
        FH_HOST_EQ_D_D_D_DB,HTML_IMAGE_ONLY_
20,HTML_MESSAGE,HTML_SHORT_LINK_IMG_3,
        RDNS_DYNAMIC,SPF_PASS,SUBJ_ALL_CAPS,TVD_RCVD_IP
autolearn=no version=3.2.0
```

Some legitimate messages are tagged – how can I deal with that?

You can adjust the threshold at which you filter UCE, as described in the previous section. However, if you receive messages from particular senders that are repeatedly treated as UCE when they are in fact legitimate, you can tell the mail system not to scan messages from those senders.

To do this:

- Visit www.staffs.ac.uk/spamprefs and add the addresses you need, one at a time, in the section headed 'Whitelist a new address'.

- After you click 'whitelist', the address will appear in the section above, headed 'Addresses currently in your whitelist'.
  This will prevent messages from these senders being tagged as possible spam, but they will still be checked for viruses and rejected if one is found.
  Note: this facility is currently available only to members of staff.

Can I do something more than just choose a single threshold?

Yes, provided you set your Rules in the right order, you can be quite sophisticated. Apart from Rules to deal with particular senders, mailing lists and so on as described above, you could choose to set multiple thresholds filtering to multiple folders, something like this:

> Apply this rule after the message arrives with:
> **X-SU-MailScanner-SpamScore: sssssss** in the message header.
> Move it to the **'Almost Certainly Spam'** folder
> and stop processing more rules
>
> Apply this rule after the message arrives with:
> **X-SU-MailScanner-SpamScore: ssss** in the message header
> Move it to the **'Probably Spam'** folder
> and stop processing more rules
>
> Apply this rule after the message arrives with
> **X-SU-MailScanner-SpamScore: ss** in the message header
> Move it to the **'Borderline Spam'** folder
> and stop processing more rules

And here again you could adjust each of these thresholds to suit the messages you get.

I still see some offensive messages in my Inbox – what more can I do?

The SpamAssassin system and the Rules described above to take advantage of it are additional to the facilities already present in *Microsoft Outlook*®.
This means that you can also set up your own Rules within Outlook to filter on particular words or phrases.

You can also choose how strict the spam checking done by the central mail system is, via the 'spamprefs' web page mentioned above.

Where to go for more help or information

Contact Customer Services on:

t: 01785 (35)3800
e: 3800@staffs.ac.uk

All Microsoft ® product screenshots and references are used by permission of the Microsoft® Corporation Windows® operating system