



c360 Email Marketing for Microsoft Dynamics CRM 3.0

Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spamming is economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high.

False Positive is an email that has been incorrectly identified as spam or unsolicited commercial email, when in fact it is not.

How spam filters work

If you send email campaigns long enough, you will inevitably run into spam filter issues. Statistically, you can expect that on average 10-20% of your emails will not be delivered to the expected recipient because of overzealous spam filters.

It is not just spammers that get caught. Innocent email marketers who send valuable, permission based mail to people who request them can also fall into the False Positive trap.

In order to overcome the issues of spam filters it is important to understand how they work.

In broad terms, spam filters look at a long list of criteria in order to judge whether or not an email is junk. For example they might look at Spammey words or phrases such as FREE, OFFER, CLICK HERE. Each individual phrase will be assigned a spam score; some criteria get more points than others.

For example SPAM ASSISSIN would allocate the following scores:

- Talks about lots of money 193 points
- Describes a breakthrough 232 points
- Mortgage offer 297 points
- Why pay more 1.249 points
- Money Back Guarantee 2.051 points

Therefore if your overall campaign exceeds a certain threshold, your email is delivered to the junk mail folder. Unfortunately there is no black and white answer to where this threshold lies. Each server is different and it depends on the settings by the individual who set up the spam filters or the ISP who is responsible for personal emails.

c360 has invested in building a range of services that not only help you avoid getting caught in spam filters but also help improve the look of the campaign when it is delivered to a range of different Inboxes.



However before you use the c360 Email Marketing tools there are a number of common mistakes that people make when preparing campaigns. Avoid these and save yourself additional work.

- Heavy use of images
- From Name not being an Actual Name
- Watch your email frequency
- Use of Spammy phrases such as click here or exclusive offer
- "Over use of punctuation !!!??
- USING CAPITALS IS LIKE SHOUTING AT YOUR CUSTOMERS
- Block colouring of text
- Sloppy HTML coding
- Sending to multiple people at the same company in a single campaign
- Designing HTML in Microsoft Word and exporting the code
- Avoid Spam peak periods as filters tighten up
- Segment the list to increase relevance
- Check the tracking to know if you have a problem
- Insert a safe sender link at the top of your email

False Positive filtering – USA vs Europe

In 2006, European ISP's achieved a rate of 0.075 compared to a US average of 3.29 of False Positive filtering mainly because the Spam filtering tends to be stricter, also affecting legitimate emails.

ISP Deliverability

Perhaps the biggest issue for email marketers, particularly those who deliver campaigns to consumers rather than businesses is to get round the spam filters of the leading ISPs. Contrary to popular belief, it is not only the email content that generates the highest spam scores.

The two main issues which can easily be identified by the c360 deliverability service are:

1. Heavy use of images
2. The from name composed of numbers or symbols rather than an Actual Name.

Statistics

Not only do they create high spam scores, they also render poorly in most inboxes. If you analyse the top 20 ISP's in the US and Europe, you will notice that there is a strong variation in both Gross Deliverability and delivery to Junk Email folders.

In the US for example gross deliverability across the top 20 ISP's runs at 83.88%, with the top 3, IWON at 96.97%, Yahoo! at 94.80% and Gmail at 94.65%. However if you consider the same statistics by the proportion that get delivered to your inbox the average is 74.57% the top 3 being CompuServe 88.08%, AOL 87.73% and Juno 87.07%.



The reverse of this is that the highest delivery to Junk mail includes Gmail at 27%, Yahoo! 18.67% and Hotmail 16.16%.

The picture is similar in Europe with the highest delivery to junk mail being from Orange UK 28.82%, Hotmail UK 21.68% and Yahoo UK 18.85%. However overall deliverability by European based ISP's ranks higher than their American counterparts by almost 7%, with all of the top 10 ISP's delivering over 91.7% of permission based email and 94% of that going to the Inbox.

Deliverability Services SPF records and Sender Id

More and more email services and spam checkers are starting to use email authentication in their filtering processes. There are currently two protocols in use that aim to achieve this. These are the 'Sender Policy Framework (SPF)' and Microsoft's SenderID framework.

Both of these protocols work by looking up a special entry in the DNS record for the domain that the email claims to have been sent from. The special entry known as an SPF record provides information about which mail servers are authorised to send mail on behalf of that domain.

We have added an SPF record to the ecommzone.com domain that identifies our authorised mail servers. For systems using the Sender Policy Framework (such as Google Mail), this is good enough and all mail sent from our servers will pass the authentication test.

However for systems using SenderID (such as Microsoft Hotmail) customers will also need to add an SPF record to their domain. The reason for this is that email messages generally have at least 2 from addresses. Sender Policy Framework uses the 'return-path' address which isn't shown in the email client and is used for routing between mail servers and for bounce notifications etc. This will always be <customerid>@ecommzone.com for mails generated by our servers. Since we have an SPF record at ecommzone.com everything is fine. The other email address is the 'From address' that the recipient sees in the mail client.

This address is generally the customers own domain eg ccfc.co.uk for Coventry City Football Club. The SenderID protocol uses this address as the basis of its authentication. So for example, if a mail arrives at hotmail claiming to be from mark.davies@ccfc.co.uk, hotmail will query the domain name system for any SPF records setup for the co.uk domain and will check that the originating mail server (ecommzone.com) is authorised to send on behalf of that domain. We recommend that all customers using c360 Email Marketing Professional apply for an SPF record to be added to their domain(s) that they send email from (or use in the from address) and add ecommzone.com as an authorised sender.

This can be done using an include clause in the SPF record. Here is an example of such an SPF record:

```
v=spf1 mx include:ecommzone.com ~all
```

Setting up an SPF record will not automatically mean that your mail will not be scored as SPAM, the content will still pass through spam filters, but a pass result from an SPF test reduces the overall spam score and ensures that the mail does at least make it through to the next layer. As more and more email vendors take up these authentication protocols it will become essential.



Further information on Sender Policy Framework can be found here:

<http://www.openspf.org/>

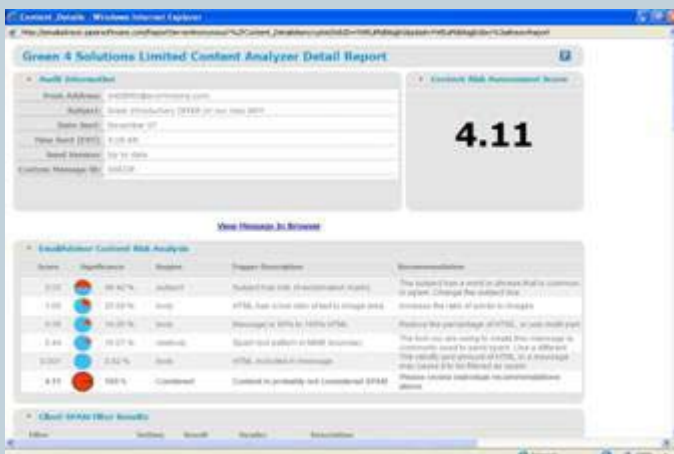
and for Sender Id:

<http://www.microsoft.com/senderid>

Content Analyzer

Despite the suggestions that are made in the previous sections of this document, and yes, both reviewing your content and using the protocols described above will help, the content that triggers spam filters is not always obvious.

Content Analyzer tests your message for spam triggers and advises you of possible problems before you send your campaign. It also checks for issues in the email header that you do not even realise are problems.



c360 Content Analyser will test your message against more than 30 different spam filters. You will receive notification once the limited report is ready. (Please note that this can take up to a few hours so try and run it in advance of your campaign). Most of the filters we check against will use a recognised scoring system to indicate the spaminess of your message. Some even indicate which elements of your message are most representative of unsolicited email.

Key Benefits

- Checks your message for attributes, keywords, and content associated with SPAM
- Enables you to modify text, links, or other message elements that are likely to set off anti-spam filters and block your mail
- Provides comprehensive coverage by evaluating your message against more than 30 different filters such as Spamcop.net and McAfee SpamKiller
- An integral part of the communication execution process



Inbox Snapshot

You have just spent hours perfecting the design and layout of your latest HTML eCampaign. It looked fantastic in the design tool and even when you sent it to your own Outlook client, but how compatible was it with the dozens of different email clients your list members use?

Certainly as part of your own good housekeeping you should send the campaign internally to check for layout and content errors. It is always best to get a second opinion. But have you got the time and resources to set up every email client that your customers use....Google mail, Yahoo!, MS Outlook, Hotmail, AOL, Demon, NTL World.

The Inbox Snapshot component of c360 Email Marketing makes this process so easy that you will be able to check your message for email client compatibility for every campaign.



The c360 Email Marketing “Inbox” option sends your email to “seed” accounts. Once the emails are delivered and the results received, Inbox Snapshot generates several reports. One shows you how your email will render in each of the over 50 email clients we test against. Inbox Advisor will also display the HTML, spell check it, show you where your message may have issues so you can correct them before you send to your entire list.

The key differentiator of the c360 service is that this function is provided as an integral part of the campaign execution process.

Key Benefits

- The only automated, integrated and real-time email client compatibility tool currently available!
- Highlights any HTML formatting problems your message may have so you can make corrections and mail to your live list with greater confidence
- Covers over 40 different email clients, including Outlook, AOL, Yahoo! and Hotmail
- Shows how your message looks in both the “preview” and full reading panes
- Checks your spelling and the validity of your HTML and hyperlinks so you don’t have to do so manually
- Fully integrated part of the campaign execution process