

THIS ARTICLE
ORIGINALLY APPEARED IN

database
marketing

Database Marketing is the only UK magazine that covers the tools and techniques used for both business-to-consumer and business-to-business customer management today. Every month, it addresses critical topics like customer retention, profiling and segmentation, data selection, site location and campaign management through a combination of regular software reviews, articles and opinion. If you want to know more about tools like data cleansing packages, OLAP analysis software and GIS, this is the magazine to read.

Not afraid to mix data warehouses with targeting or statistics with geodemographics, *Database Marketing* bridges the gap between sales, service, marketing and IT to inform both those that work directly with these tools, techniques and data, as well as board level executives that have to decide which systems and services to choose for their company.

Why not register for a free trial copy?

For a sample issue:

Contact 0845 686 0125 or email
info@dmarket.co.uk.

Visit www.dmarket.co.uk for more
information and to register online.

Robert McLuhan discusses how to make it past the spam filter to the inbox and finds that if you're not on the white list, you're not getting in.

Spam or deliver?

Email marketers expect to win sales by combining an irresistible offer with a brilliant creative, and making sure that it is properly targeted. But their efforts will be completely wasted if the message is never actually received. This is a comparatively new headache. Whereas a letter can normally be relied on to reach the doormat, getting an email into the hands of the intended recipient is an art in itself.

Assassinating spam

Around 58 per cent of the 34 billion emails produced daily are spam, according to Messagelabs, and the measures needed to deal with it are becoming ever more draconian. Microsoft says it blocks 2.4 billion junk messages to its MSN and Hotmail subscribers every day, and other internet service providers are just as active. Unfortunately, their spam filters are also thought to trap between 20 per cent and 30 per cent of legitimate marketing emails, which they fail to distinguish from the viagra merchants operating out of the US and Asia.

This puts the burden squarely on email marketers, who are effectively presumed guilty until they prove themselves innocent. If their offer has the smallest sniff of spam about it, the ISPs' guard dogs will ensure it

never makes it through the gate. Those that are emailing businesses also have corporate firewalls to contend with. So what should they do to ensure that the maximum number of emails reach their destination?

Most companies will let themselves be guided by a good email service provider, which will set up a dedicated address and ensure it is whitelisted with all the ISPs, a highly specialised activity that few businesses can afford to spend the time it requires to set up. It will also give advice about how to develop the creative and warn of what type of content – images, subject headings, key words, and so forth – may trigger spam filters.

Before a campaign, the ESP will run a deliverability audit, running the message through its filtering software to find out if there is anything in the content that may potentially cause a problem. It will also make use of software such as Pivotal Veracity and Return Path, running a test with major ISPs to check what percentage of the email actually make it to inboxes. These tools will identify the problems and what needs to be done to fix them.

One of the biggest issues will be the reputation of the emailer and its sending address or domain. Major ISPs such as AOL provide a “report this sender as

spam” button, and nothing ensures a blacklisting faster than a high proportion of complaints about your emails. This need not be a concern to reputable companies, as long as their campaign is properly targeted on an opt-in basis.

“You need to ensure that clearly marked unsubscribe messages are included in your message, and that all requests to opt out are respected,” recommends Paul Crabtree, marketing director at Adestra. ESPs regularly receive the names of people who use spam links, and suppress them to help this process, he says. It’s also worth including a reminder to the recipient to add the company name to their safe sender list or contact address book, as this will stop a junk filter being activated.

When it comes to coding the message in HTML absolute accuracy is needed. That’s because spammers give themselves away by being shoddy about it, so mistakes such as broken links or unclosed tags will quickly lead to the message being blocked. This should be one area where legitimate mailers can easily score, but in fact ESPs say a surprising number of templates created by legitimate companies are poor and need revision.

Another tell-tale characteristic of a spam campaign is the huge number of bouncebacks it generates. Spammers often mount “dictionary attacks”, bombarding major ISPs with messages created for every variation of name spelling and numbers, knowing that at least some get through. If a campaign list includes a high percentage of redundant addresses then it will look like spam and be treated accordingly.

Then there is the creative, which needs to be scrutinised for words and other features that will most likely lead to the message being blocked. Since spammers are

“In the case of one campaign we worked on recently, the key word that was triggering the spam filter turned out to be the company name itself. So you need to do detailed work on this,” Marjot says.

Watch your words

A more common problem is that legitimate marketers habitually employ terms that are often also used by spam, which means they can end up being treated as such. Fortunately it is not always necessary to maintain a rigid distinction in this regard. Filters score suspect features and make a final decision on the basis of an aggregate, so it is possible to introduce a certain amount of flexibility.

Chris Combemale, chief operating officer at Emailvision, says: “Sometimes there’s a trade-off to be made between a compelling offer and maximum delivery, and you need to make a business decision about that. For instance, the word ‘free’ in the subject line might indicate a spam message, but a supermarket making a ‘buy one get one free’ offer can’t really avoid using it. In this situation, it might decide that it will make more sales by keeping the word and reaching 88 per cent of its customer base than by reaching 92 per cent with a watered-down message.”

However, it’s not ideal that ISPs can make unilateral judgements about content, and in some cases Combemale considers their behaviour tantamount to illegal censorship. If an individual has opted into receiving an email from a company, it should not be up to the ISP to decide whether or not to allow it pass through, based on a scan of its content, he insists. The problem is particularly acute with a client such as Anne Summers, a very legitimate high street business, but one whose content sometimes poses challenges.

“Their customers have every right to request information from a retailer, and an intermediary has no business to restrict it,” he argues.

Images are a powerful addition to HTML messages, and are useful in drawing the reader’s eye to text. But some filters strip them out, and if this happens, an artfully constructed email can fall to pieces. That’s especially the case where a graphic incorporates key information, such as the date and time of an exhibition that is referred to elsewhere in the message, as its disappearance can cause confusion.

“Problems with images can have a dramatic effect on your view rates but more importantly on your branding efforts. Consider how your email campaigns might look when images do not appear” says Anthony Green, sales and marketing director at Concep.

In such matters, input from a knowledgeable supplier can make a real difference. RM, a supplier of educational software, found that its messages were not being delivered to up to a quarter of schools that had opted in to receive them. This was partly because they were laden with graphics which were triggering filters,



Sometimes there’s a trade-off to be made between a compelling offer and maximum delivery

Chris Combemale, chief operating officer, Emailvision.



If someone receives two or three disappointing emails, they move you to the junk filter

Andrew Coghlan, head of strategy, Responsys.

always looking for a new ways of getting past the filters this means keeping a constant eye on them. Their most recent innovation is randomized image graphics that include dots, varying sizes and colors, and multiple animated graphics, an approach which has confused ISP’s filters and let in a huge new wave of junk messages.

Bill Marjot, chief marketing officer at smartFOCUS, says: “Our Bayesian network software is always looking at what they are saying and how, in terms of the words, tones, and cadences they use, and we incorporate that in our spam checking algorithms.” Tests sometimes reveal that apparently quite harmless words can cause problems.

resulting in them appearing in an incomplete state or being blocked altogether. When Adestra overhauled the HTML template and sent it via its Message Focus system there was an immediate improvement in deliverability of 12 per cent.

“Now no matter which browser the recipient uses, the emails look consistently good and reflect our brand values,” says Ian Skeels, business development manager for RM Schools Marketing.

It’s not ideal that ESPs and their clients have to constantly fiddle with campaigns to make sure they get through. Much better, one would think, would be some sort of certificate that advertises a company’s trusted status. This is the idea behind Microsoft’s “bonded sender program” for Hotmail and MSN, which works by an organisation putting down a bond to guarantee good behaviour.

All emails that are sent out are digitally signed by the sending server to say they conform to this scheme, which gives them white list status. For every one that breaks the rules, a small amount is taken from the bond, effectively like a fining system.

Another approach is being tried in the US by Yahoo and AOL, whose Goodmail system guarantees the delivery of bulk emails for a fee of \$2 to \$3 per thousand, bypassing their standard filters and ensuring the images are properly displayed. Here too there is a clear advantage: once a company has been accepted, it can sail through the gates as well as offer reassurances about its *bona fides* to the recipient.

Goodmail is coming to the UK, and with BT said to be planning to sign up is being taken seriously by several ESPs. However unless or until other major ISPs sign up it will cover barely a third of the global market, which somewhat limits its appeal to advertisers.

There is also concern about the extent to which businesses are prepared to pay for a delivery channel which so far has been free. This may not bother financial services, which urgently need to distinguish themselves to customers from the fraudsters who write in their name seeking bank account details. But the premium price might be onerous for small to mid-size businesses, and in the US has been vociferously resisted by charities.

Another consideration is that to be effective such schemes have to limit themselves to the whitest of the white. Goodmail’s threshold for acceptance is a complaint rate of under one per cent and, perhaps unsurprisingly, initial applications to join the scheme tended to come from companies that cannot come close to that. In the meantime, the organisations that rigorously follow best practice may consider that they do well enough without needing to add more costs.

Many marketers consider a successful delivery any message that does not result in an automatic bounce-back and where the recipient has not unsubscribed.

But treating unsubscribes as a metric is becoming questionable, as consumers are more and more wary of interacting in any way with unsolicited mail for fears that their identity and bank account details are being “phished”. Instead they play safe by diverting it to their own junk filter.

Building opt-in

Reports by AOL and other ISPs suggest that for every message that bounces back, three meet this fate. “That is a very worrying statistic,” says Andrew Coghlan, head of strategy at Responsys.

Coghlan points out that the generic emailing from overseas is merging in consumers’ minds with email even from organisations that they have opted into. “If someone receives two or three disappointing emails, they move you to the junk filter, and once you are in there you don’t get out,” he insists.

The answer, he believes, is to persuade recipients that there is a benefit to receiving emails, in which case there will be relatively few problems. This involves building a solid opt-in list based on a motivating value proposition. Ideally this would mean creating a preference centre where consumers can opt in or out of different communications. This ensures that they only ever receive what they can make full use of from a particular brand, and reduces the likelihood of them consigning it to oblivion.

Legislation requires consent from consumers to receive emails, but Coghlan is unsatisfied with anything less than a double opt-in, where potential recipients give their address and receive a message containing a link which they can activate as confirmation. “Best practice is to be absolutely clear what you are going to get, which means an initial quick sign-up followed by an opportunity to check out both your privacy policy and previous communications of the type you plan to send.”

If this all sounds a bit too much like hard work, Coghlan argues that too many companies are interested merely in short-term sales from email campaigns and neglect the channel’s ability to make or break a relationship. “When people are pleased about getting 30 per cent open rate on emails, ten per cent click through and three per cent conversions, I point out that they are potentially alienating the other 70 per cent,” he says.

Deliverability is a large and complex topic, and probably not one that many marketers want to get too closely involved with. As with data and other technical issues, that is not necessary, as long as they pick a reputable supplier and closely follow its recommendations. What they should be in no doubt about is the extent to which successful delivery can affect campaign success, and the importance of optimising their procedures to that end. ■



You need to ensure that clearly marked unsubscribe messages are included in your message

Paul Crabtree, marketing director, Adestra.