

Top 10 Delivery Tips for 2010



Mickey Chandler
Whizardries, Inc.

About the Author



Mickey Chandler has a Bachelor of Arts degree in Government from Angelo State University, a certificate of completion from the Legal Assistant Program of the University of Texas at Austin, and a Masters of Science in Computer Information Systems from Texas A&M Central Texas.

He got into technical work due to his annoyance with spam, or junk email. Instead of just deleting it, he learned how to find out where the spam really came from and shut the spammers down. His voluntary spam-fighting led to a job fighting all kinds of Internet abuse.

Mickey served as the Director of ISP Relations for Informz, Inc., an email service provider in Saratoga Springs, NY, from September, 2005, until December, 2009. He now serves as the President and CEO of Whizardries, where he is also the chief consultant for deliverability, ISP Relations, and email regulatory issues.

Mickey and Whizardries can help you with spam problems, maximizing email delivery, avoiding issues with spam filters, ISP and DNSBL remediation, setting up whitelisting and feedback loops, and other technical issues.

Contacting Mickey

To see how Mickey Chandler and Whizardries, Inc., can help with your needs, you can call him at 936-657-4858, or [visit Whizardries on the web](#).

Table of Contents

An engaged list is paramount to email marketing success in 2010.....	1
A diversified message stream is less likely to suffer from fatigue.	1
Make client communication a two-way street.....	2
Get to know your recipients.....	3
Offer content, not marketing.....	5
Test, test, test.....	5
Authentication will continue to play a major factor in delivery decisions.....	6
Send mail using consistency.....	7
IP-based reputation still matters.....	8
Take responsibility for what gets sent.....	9
How Whizardries can help.....	9



An engaged list is paramount to email marketing success in 2010.

In years past, it was possible to engage in a "batch and blast" process, wherein email was just pushed out to recipients *en masse*. As time has gone on and receiver systems have become more restrictive in what mail they accept, the "batch and blast" method of mailing has fallen into disuse. Permission has been seen as the key to having mail accepted.

In 2010, merely having permission to send mail will become a thing of the past as well. More and more, receiving systems are considering all aspects of user engagement when making filtering and blocking decisions. The result of this new emphasis on engagement is that several old considerations will need to be rethought in the coming year.

Mail sent to users must be engaging in content. Several ISPs have already indicated that they are measuring such things as time spent viewing an email. Sending messages which are quickly glanced at and quickly deleted will begin to have a negative effect on delivery efforts as such metrics are firmed up and implemented into over all reputation systems. Relevance will prove more important than ever under the new models measuring engagement.

A diversified message stream is less likely to suffer from fatigue.

According to a 2008 survey conducted by MarketingSherpa and Q Interactive, among those who clicked on their provider's "This Is Spam" button, 25% did so because they received too much mail from that particular sender.ⁱ A 2009 Merkle study revealed that 73% of respondents who opted-out of permission-based email did so because mailings were too frequent.ⁱⁱ These are signs that over-



mailing, or list fatigue, is not only a real problem facing email marketers, but it is one that is rapidly growing in nature.

Modern social networking opportunities allow messages to be disseminated quickly and easily. While many are wondering if social networking means the end of email, the smart mailer will take the opportunity in 2010 to diversify the message streams used to get information to clients, customers, and prospects. Shorter messages may be sent via a social networking site, such as Twitter, reserving the use of email for more important, and longer, communications. The challenge will be to find the proper mix of social networking and email to maximize return on effort.

For those able to strike the proper balance, the rewards should be striking. User engagement and opportunities for constructive feedback should rise, and churn due to list fatigue should fall. This should result in an overall rise in positive reputation at ISPs and an accompanying increase in the amount of mail sent to the inbox instead of the spam or bulk folder.

Make client communication a two-way street.

Currently, many mailers send mail which views the process of client or customer communication as simply a one-to-many process. Email is viewed as being akin to standing before a crowded auditorium and giving a speech, without the burden of having to stop from time to time for applause. In 2010, mailers who continue to engage in this method of communication will find themselves more and more marginalized.

As ISPs work at creating new models revolving around user engagement, another metric that will garner much attention will be reciprocal flows of communication. Already, Google has begun



measuring this particular metric, in combination with the use of authentication, as a means of determining if images in a message should be turned on by default. Senders who have received two replies from a Gmail user will find that their images have been turned on without any need for the recipient to do anything.ⁱⁱⁱ It should be expected that over the coming year ISPs may begin to scan headers and penalize organizations who choose put their recipients at arm's length. While no one has yet indicated that they are in the process of doing this, it is one logical next step in the evolving process of gauging recipient engagement and sender intention.

As a result of these anticipated developments, certain changes to the way mass mail is sent should be contemplated. Primarily, the use of "noreply@" and any variations thereof, should be depreciated as soon as possible. It sets a tone that says that the sender does not consider email to be a two-way communication process. Additionally, the use of unmonitored email addresses may give rise to liability under the CAN-SPAM Act of 2003, if unsubscribe requests come in and are not processed.

Senders should also consider actively encouraging readers to send feedback. The use of a solid call-to-action encouraging user feedback will help to prove that recipients are engaged as they click-through or send return emails as well as provide the sender with valuable insights that will help improve the content of mailings.

Get to know your recipients.

User engagement for the mail sender will mean that the sender must have greater knowledge of their target audiences. This should largely be accomplished through the use of greater transparency.

The use of preference centers to present users with options concerning the mail they receive



should increase during 2010. Often, sending mail is considered a binary option by senders: "either we send the customer mail or we do not." Instead, sending a particular piece of mail should be considered the binary option: "either we send the customer this piece or we do not." That decision should be governed by the user's own preferences.

Email is still the primary means of communication used by consumers. Further, consumers have expressed continuing desire to receive solicited mailings at the frequency they desire. However, not many mailers have given their recipients an opportunity to state what type of mail they want to receive and how often they desire to receive it.

Because of this, the mailer is not able to segment their list at all. Because the list is not segmented, either undesired or just simply too much mail is sent and subscribers are more likely to unsubscribe, or worse, click the "This Is Spam" button.

The CAN-SPAM Act allows for use of preference centers on two conditions: (1) The use of a preference center does not require the subscriber to log-in in order to completely unsubscribe, and (2) that subscribers are given a single option that will result in their unsubscription from all lists.

Preference centers, then, should be used by mailers to the extent allowed. A well designed subscriber preference center will allow a subscriber not only to choose which segments they wish to be a part of, but will also give them the ability to adjust mailing frequency. At the very least, a preference center should clearly state the general content and frequency of that list segment. The ability for a subscriber to choose what, and how often, they receive email should be presented at the beginning of the relationship, and again at every available opportunity throughout the relationship, until they unsubscribe.



Additionally, senders should consider reading through whatever messages are received when a user unsubscribes. If they are saying things like “All noise no signal” when they leave, then they are not finding any value in what is being sent. If mailings make them feel like the sender considers them nothing more than walking checkbooks or credit cards then they will almost certainly be lost quickly. They will be more likely to stay on a list and be engaged, then, if they are treated like people whose thoughts, feelings, and sensibilities are respected.

Offer content, not marketing.

An often overlooked strategy to maximizing both delivery and return on investment for the marketing dollar spent is to stop marketing, at least occasionally. Instead, allow mail pieces to offer something valuable to the recipient for having received the mail. There will be plenty of time to upsell when the recipient reaches a website or follows through on some other call to action.

In 2010, mailers who are able to recognize that users remain in control when it comes to email are those who are likely to do well. Mail streams that consist of pure marketing material are likely to do poorly as they will be characterized by continued high spam complaints and low user engagement. On the other hand, mail that contains actual content found by the recipient to be useful or desirable will do better as this mail is more likely to score well as ISPs move to engagement models when making filtering decisions.

Test, test, test.

A perennial favorite of lists of tips for mailers is the necessity of testing. This remains no less true for 2010 than it has for any previous year. Yet a 2009 eROI study found that 37% of email



marketers are not doing any testing at all.^{iv}

As ISPs move more and more to engagement models it will become more and more important for mailers to run their own tests to ensure that the mail they are sending is timely and desired. This will require testing. Effort spent testing everything from the day of the week to the time of the day a list prefers to send mail will pay off. Similarly, effort spent testing things such as subject lines and the level of personalization in a mailing will also pay dividends.

Authentication will continue to play a major factor in delivery decisions.

For the past five years, increasing emphasis has been placed on sending authenticated email. Authentication will continue to be important to senders in 2010.

Many people consider the use of authentication to be an anti-spam measure, however, a brief examination of the history of mail authentication does not bear that idea out. Further, ISPs have not historically used the lack of authentication to make filter decisions. The true usefulness of mail authentication to an ISP comes in being able to assign a reputation to a mail stream based upon who is able to authentically claim responsibility for the mail. This allows for some portability of reputation and the resulting ability to change IP addresses without the need to "warm up" the new addresses, depending upon how the ISP has chosen to set up its reputation systems.

Currently, there are two main authentication standards in use: Sender Policy Framework/SenderID (SPF/SID) and DomainKey Identified Mail (DKIM). Despite its widespread adoption by senders and its age advantage, SPF/SID is mainly in use only by MSN/Hotmail as a validation mechanism.



DKIM is a newer authentication specification which does not yet enjoy the widespread adoption of SPF/SID. However, DKIM's technical specifications have only recently solidified to the point of making adoption worthwhile. Some receivers, notably including Yahoo!, have begun to require the use of DKIM as a prerequisite to qualification for feedback loops and whitelisting. Others, such as Google's Gmail product, are known to validate DKIM signatures on incoming mail. As a result, uptake by senders has been increasing, but validation and use of data by ISPs has been slow, despite a stated desire by systems administrators to find useful applications for the data.

Senders should anticipate that the coming year will see ISPs solidify in their support of DKIM as a more-or-less universal mail authentication solution. Senders who have not adopted DKIM as their method of mail authentication should do so this year.

Send mail using consistency.

In line with the rise of DKIM's use in making filtering decisions we should also see a continued increase in the numbers of ISPs using domain-level reputation. This will mean decisions may be made concerning what to do with a piece of mail after an examination of the "From:" field in the message.

In order to take the greatest advantage of domain-level reputation, senders should send mail consistently. That means that the "From:" address and the "Friendly From" name should be as consistent as possible. Additionally, mail users should see mail on a consistent basis. Consistency breeds familiarity. Familiarity should translate into greater comfort opening and acting on an email.

Already many mailers are being penalized for failure to be consistent in their mailing as recipients are not opening mail being sent by names they do not recognize. Worse still, many are



marking messages that they have actually requested as being spam simply due to their lack of recognition of the named sender.

Do not expect that domain-level reputation to completely supplant IP-level reputation, as that will not happen. IP-level reputation measures allow a preliminary allow/disallow decision to be made prior to accepting the entire message. Domain-level reputation measures, on the other hand, will provide a touchstone that will help make the determination as to whether the message should go to the inbox or the spam folder.

The move to domain-level reputation will also further allow for reputation portability. Merely sending the message from the same address consistently will not be useful, as spammers are already forging the from field. However, an uptake of domain-level reputation coupled with consistency in messaging header formats will enhance the possibilities and the benefits of reputation portability.

IP-based reputation still matters.

Even though the new watchword of 2010 is likely to be "engagement," and even though we should see an increase in the numbers of ISPs examining reputation on a domain level, mailers should not think that ISPs have moved away from an examination of reputation. Indeed, engagement will never truly supplant reputation, but it will serve to supplement it in greater and more significant ways as time moves on. ISPs will, at least for the foreseeable future, consider engagement to be an important indication of user satisfaction with a mail stream, and so their reputation systems will consider engagement to be a major factor in their reputation mix, but not the only factor.

In other words, all of the same things that were important at the beginning of 2009 when people



were talking about reputation will remain important in 2010. Major changes to what a mailer is doing because of a perceived "sea change" should not happen as a result of this shift. While an increased examination of engagement is likely to result in some changing to when and why mail is sent, all of the other factors that have played a role in reputation systems in the past will continue to be monitored.

Take responsibility for what gets sent.

Email service providers are able to do many things. But there are also many things that they have little to no control over. Prime among these are things like mail content and frequency. These things are solely in the control of the client. Unfortunately, as things move forward and the consequences of poor mailing practices become apparent, it is the email service provider who tends to bear the brunt of the blame for things going wrong.

Mailers who take responsibility for what they are sending will tend to do better than those who flit between email service providers when delivery rates begin to go down. The reason for this is that mailers who are willing to actually take ownership for what they are sending will also be the ones who are willing to do what is necessary to implement improvements to their processes to maximize possibilities.

How Whizardries can help.

No matter what your need may be in setting up your email program for 2010, we can help. If you need help improving your reputation or figuring out how to get to know your mail program's recipients, we can help turn the arcane bits of sending email into something that makes sense.



Here are just a few of the things we can do for you:

- Review opt-in practices for best practice and legal compliance. CAN-SPAM is just a starting point. What about the Utah and Michigan laws restricting marketing to minors? And EU data privacy and permission directives?
- Help you to resolve issues with various blacklists, and guide you on which issues don't matter or aren't worth the effort. Spamcop, Spamhaus, SORBS, Fiveten, NJABL are just a few of the many blacklists out there.
- Guide you on what steps you need to take to resolve delivery issues at specific ISPs and then reach out to those ISPs on your behalf.
- Help you set up ISP Feedback Loops to provide valuable insight into which email streams are causing the most complaints and are most likely to cause deliverability issues.
- Help you qualify and apply for whitelisting at the ISPs you care about.
- Counsel you on best practices for email authentication. DomainKeys, DKIM, Sender ID and SPF – what should you implement to ensure maximum deliverability at top B2C ISPs?
- Advise you on email certification and accreditation services like Goodmail's CertifiedEmail and ReturnPath's Sender Score Certified. Where do they help and how? Are they worth the money?
- Guide you through the minefield of content filtering. How do your messages score, and what can you do to adjust that score positively?
- Share a strong technical knowledge of email specifications and mail server infrastructure best practices, to help troubleshoot the complex issues surrounding proper message encoding, send rates, and bounce handling.

If Whizardries can help you to make sense of the arcane, visit our website at

<http://www.whizardries.com>, or call us at 936-657-4858 today.

- i Q Interactive, MarketingSherpa. (2008, March 25). *Email marketers in trouble as 'spam' definition evolves to mean 'unwanted'*. Retrieved from <http://www.marketingcharts.com/direct/email-marketers-in-trouble-as-spam-definition-evolves-to-mean-unwanted-3966/> on 1 January, 2010.
- ii Merkle releases 2009 'view from the inbox' email marketing trends report. (2009, February 24). Retrieved from <http://www.merkleinc.com/wmspage.cfm?parm1=919> on 1 January, 2010.
- iii Display images from certain senders. (2009, September 15). Retrieved from <http://mail.google.com/support/bin/answer.py?hl=en&answer=145919> on 1 January 2010
- iv eROI, (2009, July 30). *One-Third of Email Marketers Don't Test Campaigns*. Retrieved from <http://www.marketingcharts.com/interactive/one-third-of-email-marketers-don%E2%80%99t-test-campaigns-9974/> on 1 January, 2010.