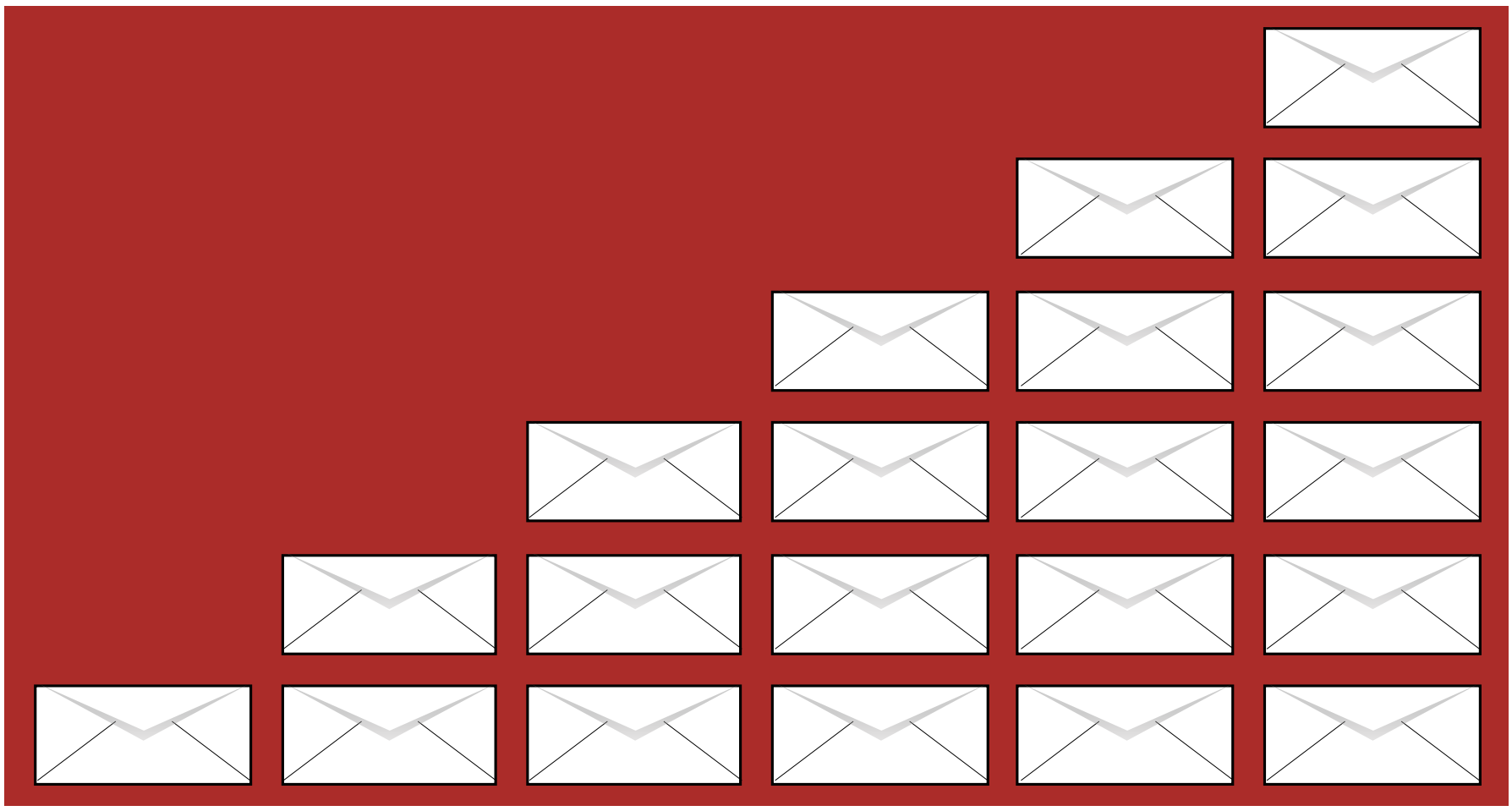
Deliverability Enhanced

Getting Email to Your Audience

2015 Revised Edition



WHITE PAPER

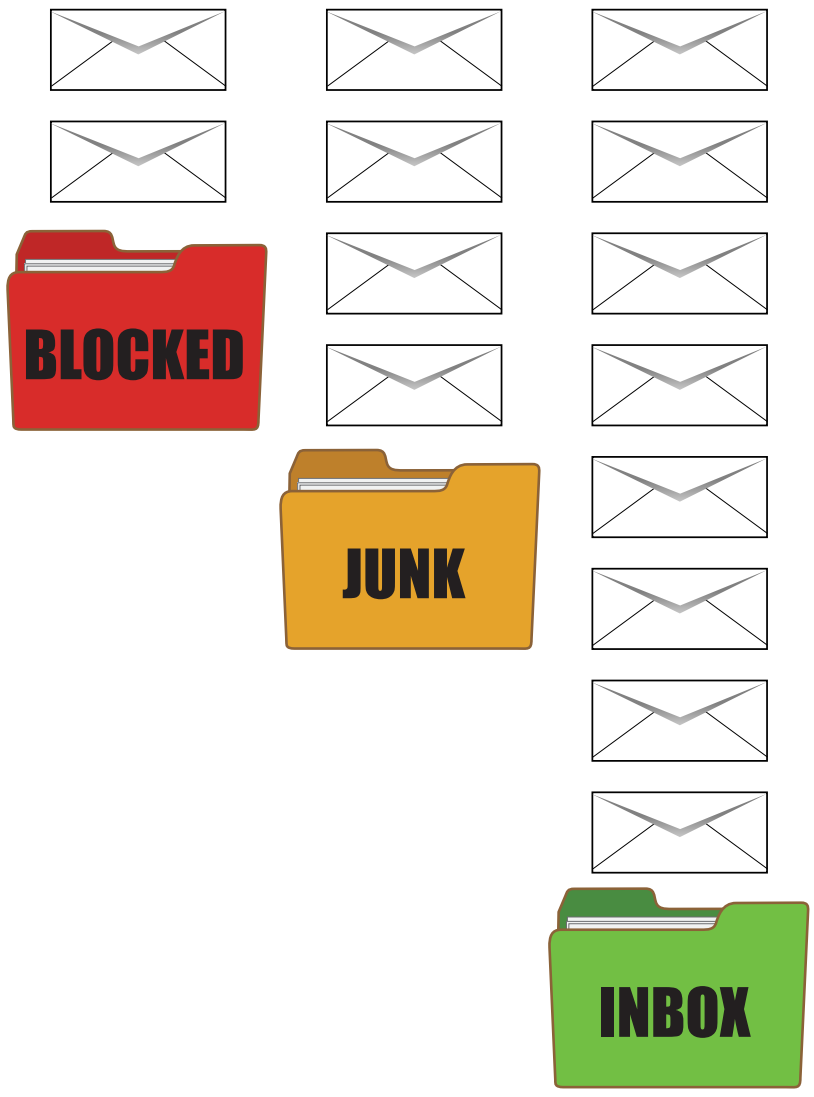
goolara

This guide is published by:
Goolara, LLC
1030 Country Club Drive, Suite D
Moraga, CA 94556
Telephone: (510) 522-8000
(888) 362-4575
Fax: (510) 522-2457

www.goolara.com

TABLE OF CONTENTS

INTRODUCTION



There is an old adage in real estate, that the three most important factors in buying a house are "location, location, location." You could apply this to email marketing as well. It won't matter if you have the best, most well-written sales copy that the has ever been written if it ends up in the wrong location. In email terms, that wrong location is the spam folder, and the right one is the inbox. Getting into the inbox may seem like an easy task. After all, the person you are sending the email chose to receive it. Shouldn't that mean it will end up in the inbox automatically? Well, no. There are many factors involved in email deliverability. Understanding these factors and what you can do to control them will go a long ways in ensuring that your emails are delivered to the inbox and read by the recipients

In the early days of email, there were no barriers in place. That important letter from your business partner landed in the same box with the offers to get rich quick. It wasn't long before so-called "spam-blocking" programs were developed. These early programs relied on identifying keywords in the subject line and the content, so terms like "diet" and "potency," or phrases like "make money now," or "earn millions," and even certain symbol combinations, such as "$$$," or multiple exclamation marks could get an email relegated to the spam folder. The problem with this approach is that anybody, from your doctor to your mother can wind up in the spam folder with just a word.

When it became apparent that certain IP addresses were often responsible for large amounts of the unwanted email, the email applications started blocking specific IP addresses. For the email marketers that were using the same IP address as the spammers, this could spell doom. While there is a movement away from the blanket ban of IP addresses, the actions of others around you can still factor into your email deliverability.

"...email applications have moved away from simple subject line and IP address blocking of the past and are looking more closely at a domain's reputation..."

Today, more and more email applications are moving towards domain-based bans, but even here, if you share that domain with people who do not use good deliverability practices, you may find yourself in hot water.

More recently, email applications have moved away from the simple subject line and IP address blocking of the past and are looking more closely at a domain's reputation. Your domain's reputation is affected by several important factors, which we will be discussing in this whitepaper. Knowing how to keep your reputation clean is the key to modern email marketing success.

A Word About This Revised Edition

Deliverability Enhanced was originally written in 2012. We've seen a number of changes in the way people create messages and how the different ISPs handle spam. In 2012, responsively designed email was a rarity. It's now quite common. There have also been some important changes in the way some email clients—most notably Gmail—handle email. To ensure that the advice in this guide remains up-to-date, we've gone through it added or modified information where necessary.

ELEMENTS OF DELIVERABILITY

Over time the big ISPs began to realize that one person's spam was another person's desired mail. Some people want to receive email about pornography, pharmaceuticals, weight-loss drugs, etc., so simply filtering the email based on keywords didn't work well. What has evolved is a system that is known as a Reputation score, where many factors are considered to produce a numeric score that controls the acceptance of the email, and its placement (inbox or bulk folder). This system is used by the big ISPs because they have the data points required to make a system like this work – they receive thousands and thousands of emails, so they can measure effectively how their users are reacting to the emails.

For B2B senders, the landscape is considerably different. They are unlikely to receive thousands of copies of the email, and a corporate mandate can override individual's preferences. You may provide your company email address to get coupons from your favorite retailer, and you may have properly opted-in, but if your company's IT department decides that coupon-laden emails from that retailer are not the best use of their email server and network, they might block that sender, no matter how legitimate it is.

The vast majority of email sent is B2C, or business-to-consumer, so that is what we will focus on right now. For more on B2B sending, go to the B2C vs. B2B section (page 21).

The Reputation Score

The Reputation score is the main factor determining what happens to your mail, so how do you establish a good reputation, and what are the factors that influence the score? Unfortunately, there is no simple answer to this question. Each ISP uses its own algorithms, and they all are constantly adjusting their algorithms based on the email flow. It is important to remember that there are people out there that are actively trying to send spam, and who are constantly

"When email is sent from an IP address that is shared across multiple companies, it is much harder for the ISP to develop a good Reputation score."

looking for new methods to get their trash delivered, so the ISPs don't reveal many details of their algorithms for fear that the spammers will find ways to exploit this information.

Although we don't know the exact algorithms and weights associated with the rules implemented by each ISP, we do have a good understanding of the main criteria that is considered. At a high level, the ISPs are able to use the fact that they have thousands of users to help sample the results and apply these to the delivery of future emails. When delivery starts, the ISPs monitor how their users are reacting to the email. If users mark certain email as spam, or delete it without reading it, the ISPs take note of this and lower the Reputation score. If an emailer's Reputation score is not very high to start with, the ISP may accept some of the mail but then start deferring the rest. This is called greylisting. With Greylisting they defer the email for several hours, refusing to accept any more, while they wait to see how their users are reacting to the email. If the user's reaction is good, the greylisting limits will be lifted, and more mail will be accepted. If not, greylisting may continue, delivery may be accepted but delivered to the bulk folder, or delivery may be rejected outright.

A Reputation score is based considerably on the IP address used for sending. It is an easy way for the ISPs to keep track of who is doing the sending. It is one of the reasons that some spammers rotate their IP addresses, burning one out and move on to another. Most ISPs are working to base their Reputation score more on the domain of the sender (and some other factors), and less on the sending IP, but the IP address is still quite important.

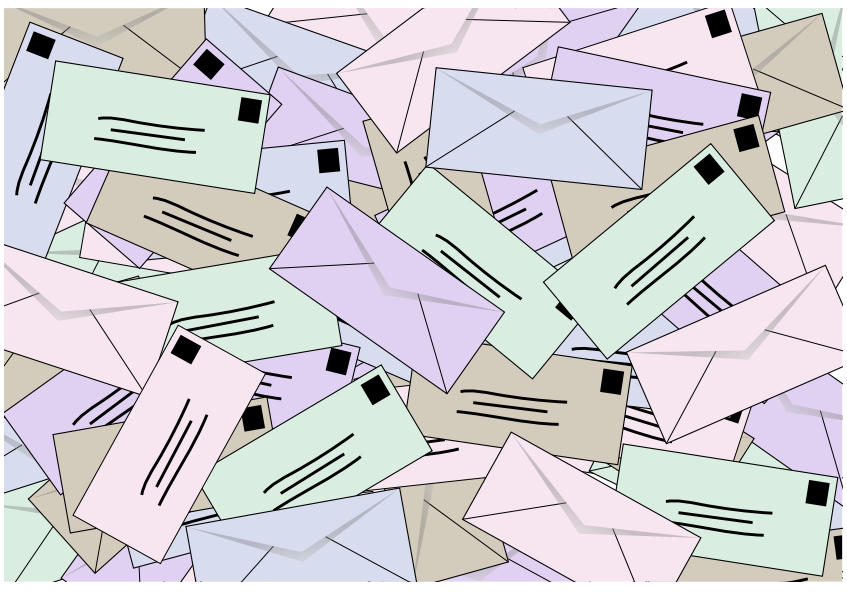
Therefore it is a benefit to the sender to have an IP address which is dedicated to their sending. The ISPs also like it, because they know that all mail sent from that IP is associated with a single company. In our experience, ISPs will offer some leeway on deliverability issues if they know the IP address is used by a single company. Getting a dedicated IP address should be trivial from your ESP, but some charge more for it, and some of the cheaper ESPs do not offer the option at all.

When email is sent from an IP address that is shared across multiple companies, it is much harder for the ISP to develop a good Reputation score. An email might be well accepted from one company, but a moment later a different company

is sending something that is generating many complaints. This means the ESP must be very concerned about spam complaints (see page 11) when sending a customer's email. Most of the ESPs that use shared IP addresses only allow a small percentage of spam complaints before they will block sending for that company. If they did not, one bad sender could suddenly cause all of the sending on that IP address to be put into the bulk folder or rejected, which would be very bad for the other customers of the ESP.

What does shared IP addresses mean for you as a sender? It depends on the quality of your list. Since the ISPs have to take an average of the email they receive to determine the Reputation score, you can benefit or be punished based on how good your sending is compared to the average. A sender with a poor quality list and poor engagement may benefit from shared IP addresses, since that mail may be difficult to get delivered. On the other hand, a good sender who has an engaged audience will not get as much mail into the inbox as if they had their own IP address because they are being pulled down by the average.

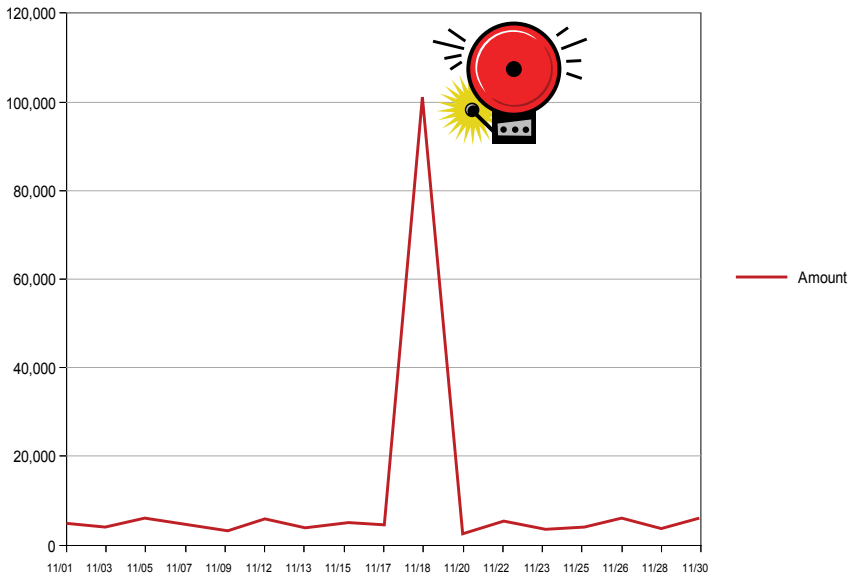
Sending Volume



As mentioned previously, one of the ways the ISPs can accurately gauge the quality of the sender is by looking at the reaction of their users over time. If the volume of email is low enough that it doesn't provide good sampling statistics, the ISPs may be unable to determine an accurate Reputation score. Determining the volume cut-off is difficult, but 10k messages/month is on the low side. With 50k/month or more the Reputation score will be more completely established.

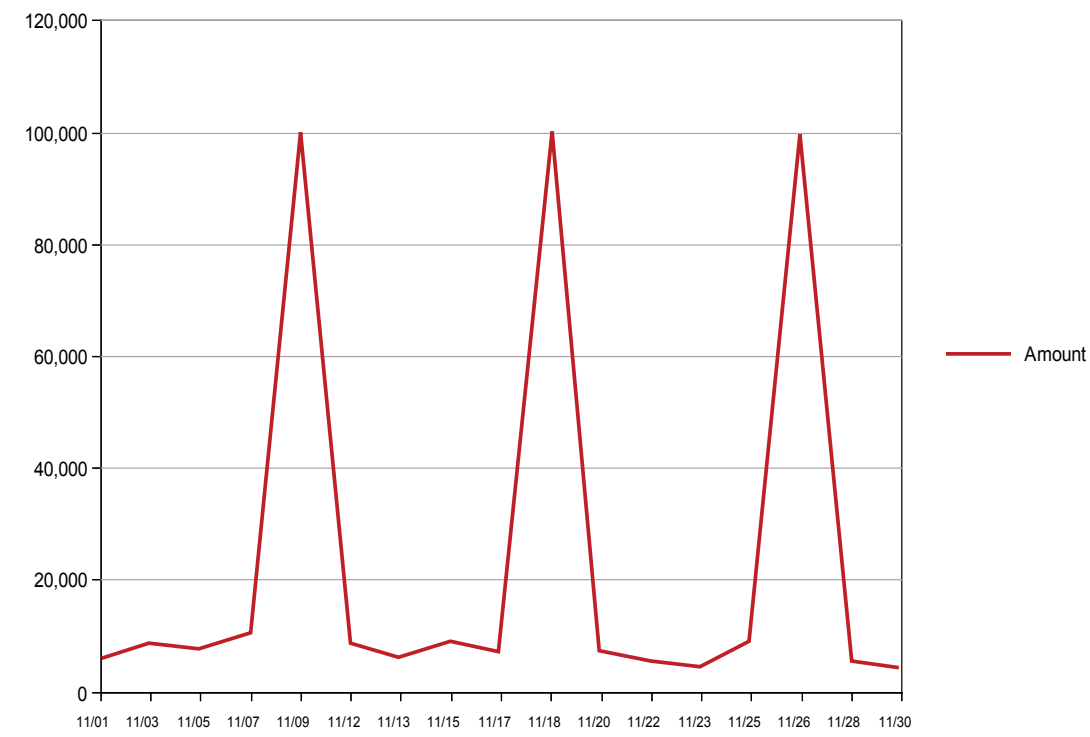
The ISPs keep the sending metrics for around a month. They have a huge number of senders to deal with, and storing this information alone takes quite a bit of storage. With this in mind, it is best to plan to send at least once a month to maintain your Reputation score.

Sudden, unexpected spikes in sending can also affect the score. Spammers will try to flood an ISP with emails when they find an opening, probably hoping to get as much delivered as possible before the ISP can determine they are



a spammer and shut them down. ISPs react negatively to these irregular changes in delivery frequency, with "irregular" being the operative word here. Besides using keywords, text-to-image ratios, bit.ly link redirects and a myriad of other ways to assess if an email is possible spam, ISPs and other mailbox providers also use your mailing patterns to identify when something's wrong. If you suddenly decide to send out 100,000 emails, where you have previously been restricting your mailing output to a few thousand, you might find your mailing suddenly throttled way back on its delivery. Sudden spikes like this can cause even well-established companies to experience delivery problems. Email marketing programs that otherwise do not have deliverability issues will see their mailings blocked or greylisted when the volume of delivery jumps suddenly at irregular intervals. This doesn't mean that a one-a-month sending is not going to get delivered, but it does mean it will face more challenges.

It's okay to have spikes in your mailings as long as the occur at fairly regular intervals. You may have some problems the first time it happens, but if you do it regularly, most email service providers will adjust and allow more of your email through in the future. Caution is always the best approach. Either send it out a little early, or make sure you have a policy in place if the mailing gets delayed. Even this might not help, though. While most ISPs throttle back the delivery of sudden, unexpected sending spikes, some ISPs will block a mailing completely if



they feel the sudden spike is suspicious. Spreading the mailings out over a few days can also help avoid problems associated with a sudden spike in mailings. Then over time, if you keep your mailings on a regular schedule, you can consolidate these mailings into once mass mailing without difficulty. The window for most ISPs is about a month, but even monthly volume spikes will cause problems. A weekly spike has a better chance of getting through. Likewise, a regular pattern, such as every Tuesday, will work better than mailing spikes at random intervals.

There are a number of options to help keep mail flowing on a regular basis. Symphonie features the ability to rate-limit the sending over any time period the user chooses, whether it be hours or days, and we've seen this help deliverability considerably, especially for a new IP address. It can also be useful to keep some email flowing during the month for transactional email, so the ISPs are seeing some good email flowing regularly.

REPUTATION SCORE FACTORS

We've discussed that the Reputation score is the main factor to determine if email is accepted, and whether it is put in the inbox. The IP address the email is sent from also has a big influence, and the speed at which email is sent. But what other factors influence the Reputation score? Here is the list. We will discuss each of these in detail:

- Authentication technologies (SPF/Sender ID/DomainKeys/ DKIM/DMARC)
- Unknown user rate
- User complaints
- Text-to-image ratio
- Keywords
- The reputation of the links
- Attachments
- Deleting without reading
- Address book entries (whitelists)

Some of these factors are much more important than others. It's possible, for instance to continue to get good deliverability with a poor text-to-image ratio, while a bad link reputation will almost certainly put you in the bulk folder. The algorithms used by email clients and ISPs are a great deal more sophisticated than they were even a few a years ago. It is possible for an email to have potential warning flags in nearly all of these areas and still land in the inbox. So many factors come into play nowadays that the old advice, such as don't use the word "save" is no longer valid. It is more important to remember that email deliverablity is a percentage game, so the fewer potential red flags you have in your mailing, the more likely it is to reach the intended recipient. It is also possible with a Reputation score that is just on the edge on acceptable to have any one of these factors tip it over the edge. That doesn't necessarily mean you should

"No authentication is likely to have a small negative effect on the Reputation score, whereas confirmed authentication is beneficial."

avoid that one thing in the future, It more likely means you should work on improving your overall score. The information in this section is primarily aimed at the B2C mailings. B2B deliverability brings its own set of rules, which will discuss in detail in a later chapter.

Authentication Technologies

When email was first created the authors had no idea where the technology would eventually lead, and to what extent email would become such a ubiquitous application. They didn't anticipate problems like spamming and phishing, and therefore the design of email assumed the best behaviors of people. When sending an email message the author indicates who it comes "from", and there isn't anything built into the mechanism of email to verify if this is true or not. This has allowed criminals to impersonate companies that have good reputation in the community to try and fool recipients into providing account or credit card numbers.

Several years ago two companies, Microsoft and Yahoo, devised strategies to allow receiving email servers to determine if the email is really being sent by an authorized representative of that domain. But that led to the first problem: How can you know who is authorized to send "as" a particular domain? The answer both companies settled on is that the Domain Name System (DNS) could be used for this. A domain only exists on the Internet if it is in the DNS, therefore, any company that can control the DNS records for themselves should be able to indicate who is authorized to send "as" that domain.

With both protocols, the mail receiving server receives enough of the email to get the "from", and then makes a request to DNS to see if records exist that indicate who is authorized to send as that domain. Failure to find a record indicates that delivery should continue, ignoring this step. If a record is found in DNS the specifics of the particular protocol are followed to check if the machine sending the email is authorized. The instructions in the DNS record can indicate what action the server should take if the mail is not authorized, but if the instruction is not to reject the email there is little point in implementing the technology.

SPF

The first company, Microsoft, created a protocol called Sender Policy Framework (SPF) that allowed the IT administrator to indicate all allowed mail servers for the domain. A record was put into the DNS with specific keywords to indicate which servers were authorized by that company to send email. This technology covers all email servers for the company, so one entry can cover an entire company that has dozens of email servers. While that is generally a good thing, it is also a downside to SPF. Some companies have mail servers throughout their organization. For their IT department to find and identify each one can be quite challenging. Some big companies have given up on this and don't publish SPF records. An additional advantage of SPF is that it doesn't require any changes in the mail sending server, as the responsibility for checking for authorization falls on the email receiving server.

In the case of Microsoft and their HotMail, Live.com, and now Outlook.com email domains, in order to become part of their sender program you must have SPF or Sender ID records published. They also made Outlook, the popular email client software, display a message at the top of the content warning recipients if the sending domain does not sign with SPF/ Sender ID records. The message appears something like "Sent by xxx@example.com on behalf of xxx@yourdomain.com". This message is useful, at some level, to know that the sender may not be authorized, but it is quite confusing for most users. Therefore we recommend that you always publish SPF/Sender ID records to avoid users seeing this message.

DKIM

The second company, Yahoo, created a protocol they called DomainKeys. This protocol solved some of the problems with SPF, but had other issues. This protocol has the email sender modify the outgoing message to create an encryption signature which can be verified using standard public/private key encryption technologies. Modifying the email message before transmission is a little tricky, and adds computational time to the sending process, but has the advantage that some

"The email marketing software should look at the results of every send and immediately remove recipients that are unknown users"

email from a company can be signed and verified, and other mail not, which is different from SPF, which is all or nothing.

Both companies submitted their designs to standards organizations, which created slightly different versions as the accepted standards. In the case of SPF the standardized version is called Sender ID, and for DomainKeys it is called DKIM (DomainKeys Identified Mail — pronounced "dee-kim"). In the case of Sender ID it appears that most companies are comfortable with the original specification and only publish SPF records. In the case of DomainKeys, the DKIM protocol appears to be more popular and fewer companies are using only DomainKeys now.

In the case of Yahoo, a sender cannot get enrolled for their feedback loop program if the email being sent is not signed with DomainKeys/DKIM. Yahoo has also demonstrated some problems with DMARC verification.

DMARC

More recently, a lot of attention has been paid to DMARC (Domain-based Message Authentication—pronounced "dee-mark"), an authentication protocol that has the advantage notifying returning deliverability information to the sending domain. While DMARC does have some interesting features, it is important to remember that it is ***not*** a substitute for SPF and DKIM. You'll still need at least one them in place to use DMARC.

DMARC's primary strength is brand protection, not deliverability. It can report back to the sending domain on every mailing, which is vital information for a business that has issues with counterfeiters. It also lets you establish a policy with ISPs when a mailing is either quarantined or rejected. Of course, DKIM already does this, so what DMARC is bringing to the table is a new, more immediate response mechanism when someone tries to use your site for phishing tactics, and another accept/reject hurdle to get past in your delivery process. For this reason, its primary value is for large companies that face regular phishing attacks. Companies in the banking services, retail, delivery, and healthcare industries should consider DMARC, as these are industries that receive a higher than usual number of phishing and spoofing attacks.

For smaller companies that are not worried about these types of attacks, but are looking to improve their deliverability, DMARC is probably not going to help. DMARC is not a simple plug-and-play solution, and, if implemented incorrectly may actually interfere with deliverability.

Summary

No authentication is likely to have a slight negative effect on the Reputation score, whereas confirmed authentication is beneficial. It seems that a failed authentication check would mean an immediate delivery failure, but for many ISPs it is just a negative factor to the Reputation score. Using both SPF and DKIM is recommended. If your company has problems with spoofing and phishing attacks, you might want to consider adding DMARC as a way to protect your brand, but not as a substitute for SPF and DKIM.

Unknown User Rate

One of the key components for a Reputation score is the rate of unknown users. An unknown user is an email address that is no longer used or was never created for that domain. When the ISPs get a request to send to an email address that is not valid, they take it as a sign that you do not know your customers well. The ISPs seem to realize that the only way to determine if an email address is valid is to try and send to it, so some number of failures must be allowed, but most ISPs have requirements that the unknown user rate does not go over a small percentage of the total or they will stop accepting the email.

Spam Traps

Over time some ISPs will take a small percentage of their old accounts that have been closed and turn them into "spam traps." Any sender that attempts delivery to one of these addresses will suffer an immediate, and significant impact to their Reputation score. Not all email providers use this technique. Google, Microsoft, and Comcast have stated publicly that they do not reuse unused addresses for spam traps. The ISPs that do will wait at least six months after an account closes to turn it into a spam trap, but some don't wait much longer.

"Too many marketers focus their effort on the attractiveness of the message and not enough on the deliverability aspects."

To avoid hitting a spam trap, the safest thing to do is not send to an address that hasn't been sent email (from a reputable system) in more than six months. In general this should not be an issue, as you should be sending to your customers on a more frequent basis than this, but if someone suddenly brings you a list of new prospects, be sure and ask when they last were sent email. We say from a "reputable system" because it is not important that the recipient be sent an email, but that the software properly records that the user is not valid and that this information gets propagated into your corporate systems. Simply sending an email from your website or other system that doesn't keep track of the delivery failures will not help you.

The email marketing software should look at the results of every send and immediately remove recipients that are unknown users (Symphonie, for instance, does this automatically, and puts the recipient "on-hold" which stops any future deliveries to that email address). Some other ESPs make the administrators define rules about when a user should be put on hold, with a common default being that after three delivery failures the recipient should be put on-hold. This is not recommended. Using this method has you send two additional times to an invalid email address, unnecessarily hurting your Reputation score. It also means that recipients are put on-hold in cases that might be just a full mailbox, or some other categorization that shouldn't stop future delivery attempts.

Identifying an Email as Spam

Most big ISPs now offer a mechanism for their users to indicate that the email is spam. Each spam complaint has a negative effect on the Reputation score. In the case of Outlook.com, having your mailing identified as spam is the most serious factor in your Reputation score, while other things, such as deleting without reading have very little impact. Sometimes, it doesn't take many spam clicks either. AOL, for instance, will start assigning a sender's email to the spam folder after the recipient has clicked the spam button twice. Most ISPs, however, recognize that many people use the spam button as a quick way to unsubscribe from something they may have previously requested. In these cases, receiving a few spam complaints may not be a serious issue for the Reputation score, but you should, of course, still monitor any spam

Case Study:

EMAIL MARKETER LOSES DELIVERABILITY WITH BAD ESP

The reputation of your domain, as expressed through your links, should not be underestimated. We had a reputable retailer move to our service from a no-name ESP, and they initially had considerable trouble in deliverability. The ISPs told us the issue was the reputation score of their links, but the company's links all went back to their website. We learned that the previous ESP had not been following good practices – unknown users were not being removed, spam complaints were not processed, etc. The company admitted that they were continuing to use this other ESP for some of their mail. After battling with this for several weeks we convinced them to stop using the other ESP and within a few days we had managed to rebuild the Reputation score which dramatically increase deliverability, opens, and clickthoughs. In this case the poor sending practices of one ESP created bad link statistics that carried over to another ESP, so do be careful about the links you reference.

reports carefully. A significant complaint rate is a quick way to get email delivery blocked from the ISPs. On the other hand, moving an email to any folder other than the spam folder is seen as a sign of engagement.

Text-to-image Ratio

Although keyword filters are not as important in determining a Reputation score as they were ten years ago, most ISPs still look through the text for keywords or patterns that indicate that the email is likely spam. The spammers know this, so one trick they started using is to put the entire message into an image. This gives the ISP no text to read to recognize the spammer. While it is becoming possible for software to read text in images, or to recognize what an image represents, it is still quite computationally expensive. Most email is sent to free email accounts, so the ISPs must keep their costs of processing email under control and therefore rarely can adopt computationally expensive processes such as reading the image contents.

Since the ISPs cannot read the images, they have adopted the Reputation score algorithms to consider email that is mostly images to be more likely to be spam. A popular metric is to consider the ratio of text to images. Generally we find that they like the ratio to be around 50-50, meaning that images are definitely acceptable, but only what there is some text around the images.

Many marketers find it more difficult to make the visual presentation they want without putting almost all the text into the image. That is understandable, as creating HTML that will layout properly with images around it can take considerably more time than building a single image. But a

marketer must understand that the ISPs are ultimately the ones in control in this process, and that a beautifully crafted image with all the best marketing messages included mean nothing if the user never sees the image. Too many marketers focus their effort on the attractiveness of the message and not enough on the deliverability aspects. When all focus is on making a beautiful image, the deliverability metrics suffer (as do open and clickthrough rates). A marketing person must ask themselves what would be worth the tradeoff between an 8% open rate with a beautiful image, or a 16% open rate for content that has a better mix of text and images, and still manages to get the marketing message across.

Keyword Filtering

We've discussed how keyword filtering is not used nearly as much as it once was, but it is still a consideration. Certainly keywords like "Viagra" or "save $$$" can definitely land you in the junk folder with certain mailbox providers, but the ISPs have gotten better about recognizing the type of content that you regularly send, and then accepting keywords in that content area. As an example, we send email for some pharmacies. Pharmacy spam is still a problem today, and the ISPs heavily filter for keywords in this area. But our customers have established good Reputation scores, and now can send out content that references many "dangerous" pharmaceutical terms and still get great deliverability, open, and clickthrough rates.

Our advice for keywords in general is to not worry about them, except for the obvious offenders. Unless your sending email for Pfizer Pharmaceuticals, we wouldn't recommend using "Viagra" in a subject line, even in jest, but don't worry about using "sale" in the subject line.

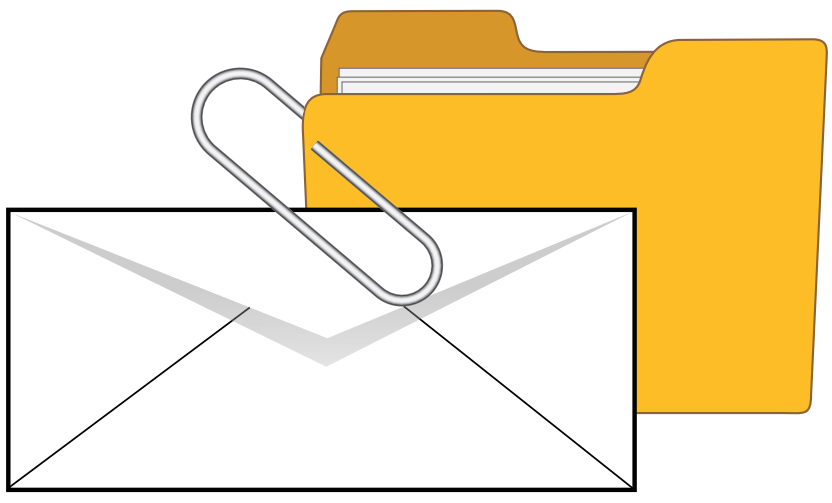
Link Reputation

The ISPs are getting better about recognizing the quality of the email contents based on the link destinations in the email. Links that go to known bad sites cause a dramatic impact on the Reputation score. Generally this is not a problem for

most marketers, as you are sending the recipient to your own website, but if you have cross-promotions or other reasons to include links to other company's websites be careful that this other company follows good business practices.

By default a tracked link will have a destination of the ESP's web server as the initial link location. This means that the ISP will see all the tracked links going to the ESP, and not to the company. Better ESPs allow users to create their own DNS name that ends in their domain name but actually references back to the ESP's server. This makes the link look like it is on the company's web server (which may be correct after the clickthrough processing), but it also gives the email recipient some confidence to click on the link, as they may recognize the company name more than the ESPs clickthrough server address. Goolara allows, and even encourages, customers to create this DNS name to increase their clickthrough rate, and does not charge for this service.

Attachments



Sending an email attachment is a quick and convenient way to get a product brochure, short video, or other content to recipients so they don't need to separately download it themselves. Goolara Symphonie has always featured the ability to send attachments, but it is another example of how spammers, phishers, and other malicious people have ruined a good thing. Thanks to the use of attachments to spread viruses, Trojan horses and worms, the recommended email protocol these days is to never open an email attachment unless it is something you are specifically expecting. Anything else stands a disturbingly good chance of being harmful. ISPs recognize this, and heavily filter or outright block emails that include attachments. Therefore, if you have a file to send, put it on your website and include a link to it in your HTML. This avoids issues with the email attachment filters and allows those recipients that are interested to get the file when they want it.

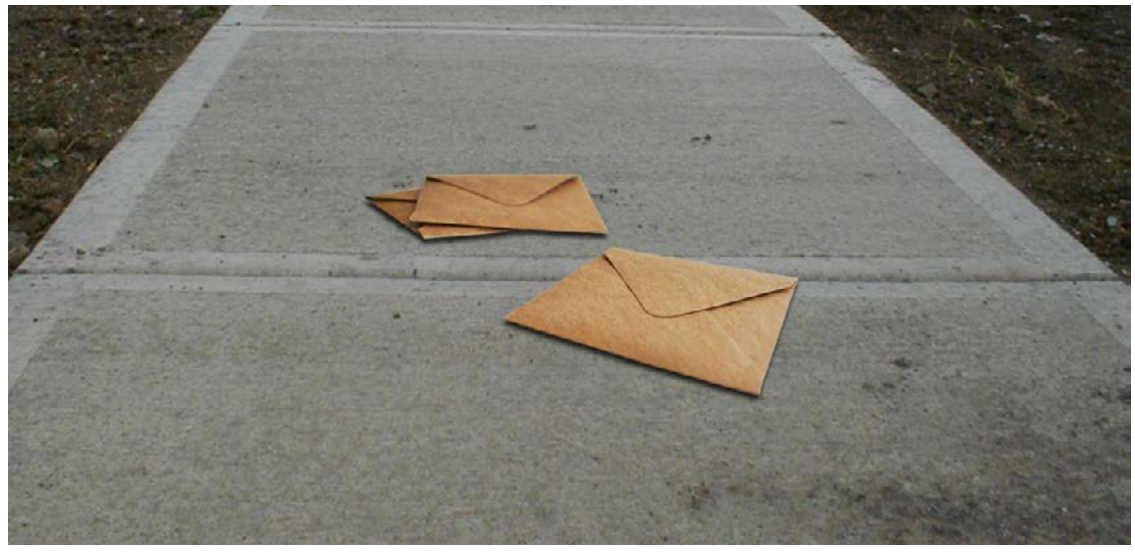
"An ISP will know if someone opens an email, even when they choose not to display the images, whereas the sender may be none the wiser"

Deleting Without Reading

One measurement the ISPs have adopted more recently is to look for the number of cases where the email recipient deletes the email without even reading it. This is considered a negative to the Reputation score.

This is a difficult issue for the marketer, as the number of people who delete without viewing is only known to the ISP, and even if the information was available, the immediate action to take to improve this is not always clear. An ISP will know if someone opens an email, even when they choose not to display the images, whereas the sender may be none the wiser. Some ISPs reportedly do not keep track of clickthroughs, citing this as an invasion of privacy. Like many of the metrics around deliverability and open rates, the important thing to remember is the engagement level of the recipients. Repeatedly sending to the same unengaged recipients will cause the ISP to assign a lower and lower Reputation score, resulting in less mail being delivered to the inbox and more into the bulk folder.

Add to this the increasingly stringent filtering methods that some email services are taking when it comes to identifying potential junk mail. Inevitably, some email that isn't actually spam will end up in the junk folder from time to time. After a while these messages are automatically deleted. Over time, if the recipient never does anything to acknowledge that they want this email, the ISPs may tag this email as unwanted, which can, in turn, hurt the sender's Reputation score. The most aggressive of the online email services is Microsoft's new Outlook.com, which automatically deletes messages from the junk folder after only ten days. This means the recipient has less time time to correct any mistaken junk folder entries than they have with most other email services.



Address Book Entries (Whitelists)

Most ISPs will consider the email addresses listed in their address book when determining the placement of email between the inbox and bulk folder. With most ISPs it is difficult to get a good measurement of the impact that having the email address listed in the address book will provide, but it is clearly some benefit. Since the recipient is clearing that address for delivery, it is one method to "whitelist" the address of the sender with the ISP.

Some marketers include a request in the email that the recipient add their address to the whitelist. In our experience this used to be more common, but seems to be falling in popularity. If you offer this advice, be sure that you use a consistent "from" address in your sending. If several different addresses are used, for different sub-companies, for example, the user's whitelist of your address will be less effective. It can also be useful to make the "from" address specific to a salesperson who is responsible for the account (a feature easily configured in Symphonie), and while this gives a better user experience, it does throw off address book whitelists, should the salesperson ever change.

ENGAGEMENT AND FREQUENCY

Some ISPs have indicated that clicks don't matter. This has been interpreted by a few in the email marketing community to mean that engagement doesn't matter, and that you can send as much email as you like to as many people as you like and not worry about whether anyone reads it. In reality, it means nothing of the sort. Engagement still matters, and you ignore this fact at your own peril. If an ISP sees that your mailings are going unread and being deleted without being opened, they will start adding negative points to your Reputation score. The effect may not be that big at first, but it will eventually hurt your deliverabilty. Put another way: Keep track of your unengaged recipients and adjust your sending accordingly. For more information on the best procedures for reinvigorating unengaged addresses, see *On-Going Maintenance* (page 36).

Deliverability Gets Personal

Deliverability is not a simple either/or proposition. The algorithms for determining deliverabilty have gotten so sophisticated over the years that simple suggestions such as "watch out for keywords" and "mind your text-to-image ratio" don't hold the importance they once had. Deliverability has become a very individualized process, for both the sender and the recipient. This doesn't mean that the actions of one recipient won't effect another, but it does mean that these things are weighed according to their own criteria. The email clients don't publish their information on what they use to judge an email's Reputation score, but it is reasonable to assume that the actions of some recipients will carry more weight than the actions of others.

“The algorithms for determining deliverabilty have gotten so sophisticated that simple suggestions such as “watch out for keywords” and “mind your text-to-image ratio” don’t hold the importance they once had.”

When all is said and done, engagement still matters. We may not have the same data that the ISPs have when it comes to opens, but we can usually get a good idea of how various mailings are doing by their metrics. While you may not want to remove recipients from your list simply because they are not responding, you should try to renew the connection with content aimed more directly at them. This may require some segmentation and dynamic content personalization, but it is worth the effort.

goolara

B2C VS. B2B

Whether your primary audience is business-based or consumer-based can have a huge effect on your deliverability. While most consumer email goes through the familiar email services (AOL, Gmail, Yahoo, etc.), businesses, more often, have their own servers and IP addresses and these are controlled by in-house IT departments. These departments have the ability to create their own rules for what constitutes acceptable email. Some, for instance, will block certain words that they feel are most often associated with spam. The problem lies in the fact that what constitutes a "spammy" word is utterly arbitrary and may be based on individual experiences. If, for instance, the IT department sees an influx of unwanted emails about weight loss, they may decide to block the word "weight." If your email includes this—even as part of another word (e.g., "lightweight")—you may find your emails going directly to the junk folder without any idea why.

Additionally, many IT departments are unsympathetic to their employees who want to use their corporate email account for non-business purposes. So even though the employee requested email coupons from some business, the IT administrator (or company policy) may have that email rejected because it is not related to the business of the company.

On a business side, most email will pass though proprietary systems before getting to the inbox of the recipient. There are a number of these systems, including names like Postini (now part of Google Apps), Barracuda Networks, and Exchange Online Protection (Microsoft Forefront Online Protection for Exchange) that mostly use keyword-based algorithms to filter the mail. In some cases they will take feedback from IT administrators or even users, with functionality for "this is spam" much like the big ISPs offer. This data is aggregated

"If an IT department sees an influx of unwanted emails about weight loss, they may decide to block the word "weight." If your email includes this, even as part of another word, you may find your emails going directly to the junk folder without any idea why."

from multiple companies to allow blocking for companies that haven't even received the email yet.

With some of the big ISPs offering low cost business plans a surprising amount of mail that appears to be going to a business address actually flows through Yahoo or Gmail. This is especially true of small businesses, but even some bigger businesses have outsourced their email to Google, so do not be surprised if a significant amount of business mail actually hits one of the big ISPs.

Since many of the anti-spam filters used by businesses must rely primarily on the keyword-based rules defined by their administrators, delivery to businesses can be quite challenging. Adding to the challenge is that many businesses are unresponsive to requests to be unblocked or whitelisted from deliverability services.

If your market is primarily B2B you need to watch more closely the words used in your email, and some of the other rules that would be important for B2C delivery can be ignored (such as text-to-image ratios).

Determining a Spam Score

It would be great if marketers could send their email through software that would tell them a spam score and specific recommendations of what to do about it. This might be more possible on the B2B side, especially if you knew the software used by the company you want to target, but on the B2C side it is quite difficult. As we've discussed, the big ISPs base more of their Reputation score calculations on the reaction of their users to the email, and less on the keywords in the content.

Some ESPs offer a service to create a "spam score" of the email. In our experience, most of these are using the open-source software SpamAssassin with its default settings. SpamAssassin has many sophisticated algorithms to recognize content that appears to be spam, according to the rules selected by the administrator,

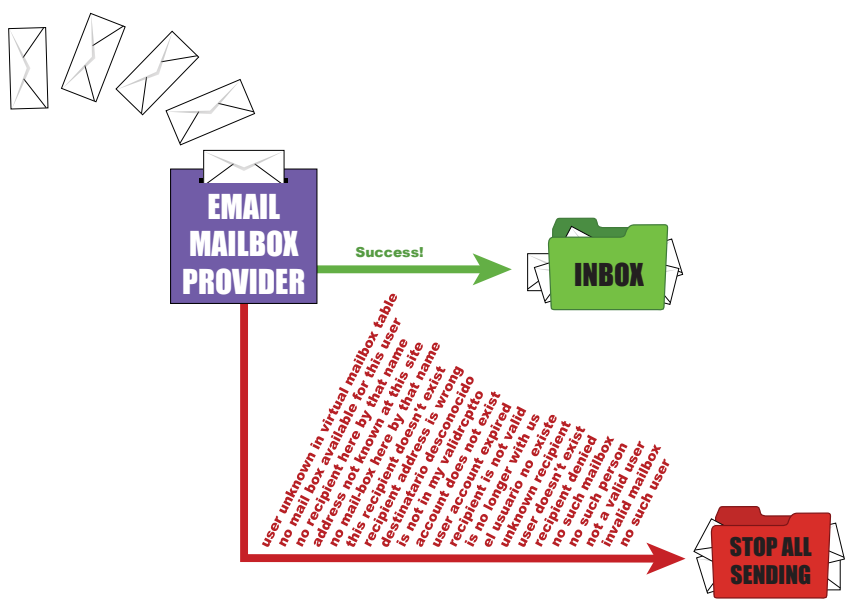
goolara

but the majority of its logic is based on keyword analysis. SpamAssassin will report how it scored an email, so you can get feedback like "subject included the word 'Sale'" as the reason for a rejection.

For this reason, we don't recommend using tools like SpamAssassin to analyze content for deliverability. We've seen administrators waste hours of time trying to work around using specific words in their content or subject line, but the end effect is a confusing email that is not better delivered to the big ISPs since they don't pay much attention to the keywords.

The best advice for getting an email delivered remains constant: Send content to recipients who are interested.

START WITH GOOD ADDRESSES



We've discussed how the rate of unknown users is a key factor in determining a Reputation score. Sending to recipients that don't exist, or who exist but don't want the email, is a quick way to ruin a Reputation score. One common cause of this is the use of email address lists that were either purchased, or culled from questionable sources. To ensure the best deliverability, the first step is to start with good addresses, and this means you need some sort of opt-in procedure in place.

Opt-in means the person who receives the email is doing so because they specifically asked to receive it. Normally this is handled as a sign-in form on your website. The sign-in procedure can either be a single opt-in or a double opt-in. Which of these is better is a hotly contested issue. Single opt-in proponents argue that you should make your potential client jump through hoops to receive your email, and that the double opt-in methods leads to fewer subscriptions, not to mention the potential for the response email to end up in the junk folder. In the opposite camp, the double opt-in proponents point to higher open rates and fewer bounces and unsubscribes. It also eliminates the possibility of someone else entering another person's email address. The single opt-in will yield more subscribers more quickly, but the double opt-in yields better results.

The sign-up form should provide details about what information will be sent (coupons, news, stories, etc.), and details of how often the user should expect to receive email. If you sent more than a few times a month it is advisable to offer the user some options of how often they will receive email. Over-mailing is a quick way to generate unsubscribes or spam complaints, so make sure your users understand what frequency they are signing up for, and give them choices if you frequently send mailings. It is better to send mail less frequently to someone who will accept it than to blast a

recipient with more mail than they want until they unsubscribe or mark it as spam.

It is key that you tell users what you will be sending, and then stick to providing that information. We hear from consumers regularly a frustration that they signed up to receive coupons, for example, but then get email about many other things, with no or few coupons.

Your sign-up page should state clearly how the email address will be shared with partners or affiliates. Ideally the language should make it clear that the email address will not be shared. Providing a link to a privacy policy is useful if your privacy policy is easily understood, and not written with too much legal jargon.

In years past there were email clients that couldn't handle HTML. Initially smart-phones also had a problem with HTML. Today these are not common issues, so there is no need to ask customers in what format the email should be sent. Some sign-up forms still offer a text-only or HTML option, but this is no longer necessary, and robs you of the opportunity to present your content in a much more visually attractive format.

BUYING LISTS AND APPENDING DATA

When a marketing person first enters the email marketing space, one of their first questions is "where can I buy my list?" In many industries buying a list is not only acceptable, it is a required action in order to move forward. Purchased address lists have been part of direct mail marketing since the term was invented. When you get home and open your postal mailbox, do you feel angry if the local pizza place has sent you a flyer? Most people don't. This "junk mail" is seen as part of life, easily ignored and thrown away. Email, however, is a different story. Since your email address is not on public record in the way that your physical address is, there is a more visceral reaction in many people to unsolicited email.

Buying Lists

Buying an email list is not the same as buying a postal list. The ultimate proof of this came in 2003, when Congress, responding to public anger over unsolicited email, passed the CAN-SPAM act, making it illegal to send unsolicited email. When recipients get emails from a business or individual that they don't want to receive, they can mark that email as spam. When ISPs get a significant number of spam complaints, they stop accepting email from that sender. Therefore, ignoring the legal issues for the moment, it is not so much a question of where you get your list, but what will be the reaction of the recipients to that email.

Some business try to get around the CAN-SPAM act through affiliate programs and partnerships. They may put language on their website that says by acknowledging you want to receive something from them, you agree to receive email from their "partners and affiliates." Then they offer affiliate licenses to companies that are interested in their lists, thus skirting the spirit of the law without actually breaking it. The CAN-SPAM act has quite serious penalties, but there has been very few news items about businesses prosecuted for violating the law.

"While it may be tempting to augment your house lists with email addresses from an outside service, you must consider the reaction of users to receiving this email."

As a consequence, it appears many senders are pushing the limits of what the law allows.

On some level, the question of an email's legality is moot. In terms of deliverability, it doesn't really matter what the law says, it's what the ISPs do. ISPs aren't so much interested in enforcing CAN-SPAM as they are in making their email client applications as appealing as possible to users. Since they sell advertising space for display in those email account windows, the more people that want to use their email clients, the more money they make. Whether an email violates the CAN-SPAM act or not is less important than the reaction of the users. If users say your email is spam, then it doesn't matter if Congress disagrees.

Since users don't react well to unsolicited emails, it makes sense that buying a list would not generate good results for email marketing. This research is confirmed by Goolara's internal studies and born out by by other studies across the Internet. Most people who purchase email lists do not get good results from them. They may get their brand reputation damaged by being identified as a spammer, or they may get their email blocked, meaning that even email that was opted-in will not be delivered. Worse, they may get blacklisted, an even more damaging status that will make it extremely difficult to get any email delivered at all.

So how can you start a business using email as your primary source for leads, or grow an email list, without purchasing a list? The answer, unfortunately, is the hard way – you need to build it organically. The best way is to offer a signup on your website, and then send recipients content they enjoy receiving. Over time the membership will grow.

Appending Lists

The CAN-SPAM act says that a business can communicate with a customer without requiring a separate opt-in. This enables email confirmations and other useful mail, but some businesses use this as a way to grow their lists without the worry of CAN-SPAM violations. However, it the same basic issue exists – sending email to recipients that don't want it leads to more complaints and unhappy customers.

Case Study:

LIST APPENDS LEAD TO MULTIPLE COMPLAINTS

We worked with a reputable business owner who wanted to target more of his customer base with email marketing. He had a large number of customers that had purchased items from him over the years, but he didn't have their email addresses. Against our recommendations, he worked with a reputable company for an email list append. They found email address for around 30% of his list, and he began sending them his regular advertisements.

The reaction was swift and brutal. Immediately his Reputation score nosedived, and soon it was a struggle to get much of his email delivered. Some of the people who had not given him their email address in the past had often done so intentionally, not wanting to receive email marketing. Now ads were suddenly coming to them, and they reacted by marking his email as spam. It is harder to measure the negative impact on his brand identity, but it certainly suffered also.

At first, he thought his tactic was a success, because he was able to tie several sales to the appended leads. However, in time it became clear that the loss in deliverability across all his customers had a far more negative impact on his revenue than the few sales he picked-up from the appended addresses. In the end we had to remove all the recipients from his list that he had added as appends. Our deliverability team had to work with the ISPs to let them know that all the appended recipients had been removed, and that the customer had promised never to do this again. After that his deliverability went back up to 99%+, and his sales recovered.

So while it may be tempting to augment your house lists with email addresses from an outside service, you must consider the reaction of users to receiving this email. If the user's decide it is unsolicited and undesired, your Reputation score and your brand image will suffer in ways that may be far more damaging than the little lift you get from some appended customers converting.

AUTOMATED PROCESSING

Good email marketing software should free the administrators from dealing with issues of bounce handling, delivery retries, spam complaints, etc. Marketing professionals have enough on their plates without worrying about forgetting to tell the email marketing software to remove the recipients who have unsubscribes or complained. Here are some aspects of email delivery that should be handled automatically, or with little configuration, by the software:

Throttling

Good email marketing software should automatically throttle the sending based on the real-time response of the ISPs to the mail. When the ISPs start responding with slow down messages, the software should adjust accordingly. If the ISP uses a greylisting strategy, the email marketing software should adjust the sending strategy accordingly. It is also useful if the software user has the option to slow down a delivery, especially when warming up a new IP address.

Bounce Handling

During the delivery process some mail will be accepted by the receiving mail server, but that server will later send an email back saying it didn't, in fact, accept the email. This is called a bounced email. The email marketing software should process these automatically, and recognize the kind of failure reported by the site. If the response is that the user is unknown, the recipient should be put on-hold immediately. If the message is more of an informative one, saying delivery has been delayed, the message should basically be ignored. If the mailbox is full or other similar status should be recorded as such, and not counted as a delivery failure against that recipient.

Unknown Users

When the email marketing software is made aware that an email address is invalid, it is important to immediately put that recipient on-hold, and not allow any further email to be sent

to that recipient. There is no reason the administrator should have to configure this process if it is written correctly. Only those responses from the receiving mail server that indicate the user in unknown (expressed in hundreds of different ways in English) should be put on hold. If the mail server rejects the email because it considers it spam, the user should not be put on-hold. If the user's mailbox is full, the user should not be put on hold. But if the message is that the email is invalid, the user should be put on hold immediately, so no further attempts are made to deliver to a bad address, as it hurts the Reputation score.

Header Unsubscribe Ability

For many years ISPs have recommended that the header of every email include the instructions of how to unsubscribe the recipient. Microsoft has taken this a step further, and will automatically process an unsubscribe based on this information in some cases. Furthermore, they require that this information be in the header to deliver to their properties (Hotmail, Live.com, Outlook.com). Symphonie automatically includes this information in the header, with no administrative involvement required.

THE SENDER'S IDENTITY

When a recipient gets an email, in most email clients, only a few pieces of information are shown for users to decide if they should open the email: the subject line (or a portion of it, if it's long), and the "from" address. Who the email comes "from" is therefore incredibly important in deliverability. We've seen how it is used in the authentication protocols (SPF/Sender ID/DomainKeys/DKIM/ DMARC) and in address book whitelisting. Now it is time to consider the user's perception to the "from" address.

Most users receive a considerable amount of email, and spend very little time deciding which ones they will open or discard. The "from" address is one of the key criteria considered, as the user wants to know who is sending them email. If the "from" is immediately recognized, it will increase the likelihood of the email being opened. It is quite likely that users will recognize an email from "apple.com", and even a subdomain like "news. apple.com" will likely be recognized, but each subdomain added to a known brand will make the user think for a moment if it is really the brand they expected, so the ideal case is to use exactly the name they are expecting.

Be careful to send "from" the brand that the customer is expecting if you have several brands under one company. For example, The Gap owns their namesake brand, plus Banana Republic and Old Navy, among others. If a customer signs up in Banana Republic to get emails, they shouldn't come "from" Gap.com or some other brand, as the customer may not recognize that these are parent companies. Good email marketing software should make it easy to support sending "from" whatever brand the user is expecting.

As we discussed under the SPF/Sender ID authentication information, failure to properly create SPF/Sender ID records for the "from" address can result in software like Outlook

"If the 'from' is immediately recognized, it will increase the likelihood of the email being opened."

displaying an "on behalf of" message that is quite confusing to recipients and causes less email to be opened.

One thing that is often cited as an example of the benefits of social marketing is that it allows the company to hear directly back from the customer. This is an interesting statement, as email has been around for far longer and allows a channel for the customer to provide feedback directly back to the company by "replying" to the email and providing their feedback. But most marketers tell the customer that they don't want to hear their comments, explicitly in the text of the message saying statements like "Do not reply to this email as it goes to an unattended mailbox", but also from their choice of user IDs in the "from" address, such as DoNotReply@ addresses.

It certainly can take some staff's time to go through the email replies, but one of the questions for a business is: Would you rather have someone's complaint sent directly to your company, or put out on a social site where many potential customers can see it? For this reason alone it seems that most companies would want to accept reply email, but yet it is an uncommon thing.

Telling customers that their opinion is unimportant sets a particular tone to the email. If you are trying to build a brand image, telling customers that their feedback is unwanted is not going to help. Just consider the emotional reaction you have to DoNotReply@ versus MyVIPClub@, for example. Add to this the inescapable fact that many recipient will, in spite of the request to not reply, will do exactly that, usually resulting in an autoresponse that might serve to alienate your audience. It is a far better approach to use a triggered email, ideally one with dynamic content capabilities, that can respond to the recipient in a more meaningful manner.

The ISPs also consider the user name in the "from" address, and appear to give a small negative adjustment to the Reputation score when they find addresses like "DoNotReply@."

MOBILE MARKETING

Every day, more and more people look to the smart phones to read their email. How is deliverability affected by sending to a mobile device? The answer is that it is not much different than most other big-ISP deliveries. Many customers will use POP (Post Office Protocol) to pull their mail from their existing provider. POP sends the email to the mobile phone, but leaves a copy of the email at Gmail, Yahoo, AOL, etc. It is possible to have a mobile-specific address such as @verizon.net, att.net, or t-mobile, for example, but most customers seem to stick with their existing email providers rather than use one from their mobile carrier.

The increase in mobile phone viewing has caused some shifts in the way people respond to the email they receive. An email that was designed without any thought for how it looks on a mobile phone runs the risk of being deleted immediately. In most cases, this isn't a major consideration, the mailbox provider will have still registered the open, and, in the case of the iPhone and some Android phones, images are turned on by default, so you'll probably get the open acknowledgment. Even if you don't the mailbox provider will have registered the open, so it shouldn't affect your deliverability.

On the other hand, you do run the rick of losing some sales due to the unreadability of your mailing. This, however, has less to do with deliverability than email design. For more information on this, see our Responsive Email Design Guide in the Resources section of the Goolara website.

THE WELCOME EMAIL

When recipients have provided their information to opt-in, it is important that you get them an email confirmation right away. This has become fairly common, so recipients will be looking in their mailbox, expecting the email shortly after the signup. ***Do not overlook this.*** If if they open that email, they will have already started the process of helping establish good deliverability since the ISP sees that email being opened. If you wait a few hours or more, recipients may forget that they signed up, and will look suspiciously at the email when it arrives. It is especially important to get an email to the user immediately if you are using the double-opt-in technology to ensure the email address is valid, as the rate of response drops quickly over time.

If you must take opt-in requests via paper or other offline source, where there is time required to data-enter the information, it is especially critical that the subject line and email content explain to the recipient why they are receiving that email. Otherwise too much of it will be rejected or marked as spam. With more and more people all over the world getting email addresses and changing these address every year or so, the complexity of the email addresses themselves is increasing. More have a strange combination of letters and numbers that can make rekeying a real challenge. Whenever possible try to have users enter their email addresses onto on-line system, using a keyboard, rather than hand writing.

Any good ESP should make it easy to get an email sent out to new recipients when they are added, so the email can be delivered immediately.

While it is important to get that first email to the customer right away, the next critical step is what to do from that point onwards. Some marketers find it useful to create "on-

boarding" programs, where the user starts a drip campaign of several messages over time that introduce them to the company and give the users key information. These can help with deliverability if the users engage with them. If they wind up being junk mail that is ignored by the users, the programs should be altered or eliminated.

ON-GOING MAINTENANCE

Here's the dirty little secret that nobody wants to talk about: you will lose some recipients over time. They may have signed up for your email, and they may even like getting it, but perhaps they are overwhelmed by the amount of email in their inbox every day, or perhaps they subscribed to your newsletter because of their job, and now they've moved to the country to raise bees. Whatever the reason, you're bound to get some notifications that your email has been identified as junk. It would be nice if everyone used the unsubscribe link in the email, but some people either find it easier to click "Mark as Spam," or they have heard that clicking the "unsubscribe" button will result in even more email (for more on this subject, see http://blog.goolara.com/2012/08/07/the-great-unsubscribe-myth/).

In some ways, the recipients who mark the email as spam are better than those who just never look at the email again. We'd certainly prefer that they unsubscribe, but at least you know they are not interested any more. A recipient who continues to receive the email (no delivery failures), but never opens or clicks is a more difficult challenge. No marketer wants to give up on an address that could convert some day, but it is important that you recognize the downside of unengaged recipients.

Remember that the ISPs determine your Reputation score based on the reactions of their users to your mail. They consider whether the recipients open the email to determine if recipients want to receive the email. When mailings are deleting without opening, message after message, the ISP will eventually decide the recipient is uninterested, which will lower your Reputation score for that subscriber, and may affect your overall Reputation score if enough people follow suit. While deliverability has become a more individualized process, this

"At some point senders should implement a "win-back" program that is designed to target the recipients who are unengaged."

doesn't mean that no one affects anyone else's Reputation score. If enough people click a mailbox's "This is Spam" button, you can be sure that it will affect the score. Likewise, a large number of unengaged recipients can cause your Reputation score to be lowered to the point that many less-engaged recipients will no longer be able to see the email because the ISP is now delivering it to the junk folder.

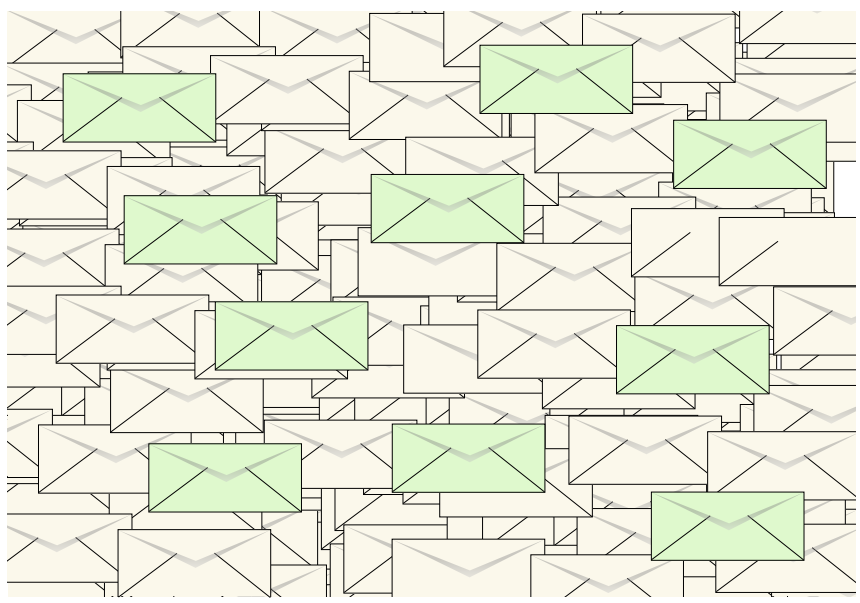
This causes a dilemma: At what point do you stop sending to unengaged recipients to make sure your emails to less-engaged recipients will still get delivered? There is no single right answer. This is something you need to consider based on the data you have available for each customer.

At some point senders should implement a "win-back" program that is designed to target the recipients who are unengaged. There are many ways to implement this, but the basic idea is to send one or more emails to those who are unengaged to let them know that they need to respond in some way or they will be dropped from the program. Those that do respond are retained, and those that do not are dropped to maintain good deliverability with the remaining recipients.

It is important to remember that what constitutes unengaged for one person might mean something else for another person. How you respond to a recipient who had been a regular customer in the past, and then suddenly stopped purchasing should be different from how you respond to the person who has elected to receive your mailings, but has never purchased anything. While the first may warrant a win-back campaign fairly soon after their disengagement was first noticed, the other many not warrant one at all.

It is a best-practice to create a preferences center for your customers to interact with. This web page should allow unsubscribes, but also allow recipients to indicate which publications they want to receive, perhaps the interval of email they desire, and perhaps a few key demographics that the company would want to know about them. Making it easy for people to change their subscription options will reduce the number who tune out completely, or mark the email as spam.

SEED LISTS



In years past, one of the best ways to measure how much of your email was delivered into the inbox (rather than the junk folder) was to use seed lists. A seed list is a group of emails included in every campaign that you use to monitor each mailing. These can be addresses for accounts you've created at a few of the big ISPs that you can check yourself, or you could have several addresses spread across ISPs that are checked automatically as part of an extra-cost service. If the delivery was successful, but the open rates seemed lower than you had hoped, seed lists might help you find out if an ISP is delivering the email into the junk folder.

However, as ISPs have gotten better at recognizing what each individual wants for their email delivery, the accuracy of the seed lists has suffered as a consequence. As we have discussed, the ISPs pay attention to the actions individual users take for their mailboxes. When email is left untouched in the bulk folder, the ISPs decide that it isn't desired. When it gets deleted without being read, they see it as unwanted. On the other hand, when email is removed the bulk folder or opened, the ISPs look at these as signs that the user wants that kind of email.

This means that the actions taken with your seed list email will influence where those emails are delivered, even when the results are completely unrepresentative of how others users react to your mail. If you dutifully remove your email from the bulk folder when it gets delivered there, and open every message, the ISPs will deliver more of your email into the inbox. You will get the warm and happy feeling that your distribution is getting all email into the inbox, but this could be misleading.

Not all ISPs are good about looking at the individual behaviors of email recipients and using that information to influence inbox delivery, but most are trying to improve. It's just a

matter of time before the individual responses out weigh all other factors. This doesn't mean that seed lists are useless, but like many metrics, you must understand that they can be influenced on a case-by-case basis. This is primarily true for the larger services, such as Gmail, and Hotmail (see page 33). As a rule, B2B deliveries do not have this level of user-based metrics, so seed lists may be more accurate for this audience.

If seed lists are not an answer to determining inbox penetration, than what is? There are two answers. One is that this might not even be the right question, as it is much more important to measure engagement of your recipients than to worry if the email is in the inbox or the bulk folder. If the user doesn't engage with the email, then it really doesn't matter where it was delivered. A second answer is to look at a report of opens by domain, which is one of the reports described in this guide to help you analyze your results. Since people don't tend to be grouped in any significant way by their choice of ISP, the opens rates should be about equal across the big ISPs. If one ISP has a considerably lower open rate, you can conclude that less mail is making it into the inbox for that ISP. Since the data on opens comes from all the recipients, not just a few selected seed list entries, the information is more accurate than looking at the seed list inbox placement.

After the email has been sent it is important to have good reporting tools to really understand how the delivery is going. Simple metrics of delivered and bounced are good for a quick view, but to drill into deliverability issues requires more information. Your ESP should normally be handling these issues for you, and bringing problems and solution to your attention, but it is good for you to know what to look for. Here is some of the data you should have available, and how to use it:

Deliverability, Categorized by Domain

All delivery failures should be categorized into 8-10 buckets of common issues. These should be categories like unknown users, mailbox full, marked as spam, greylisted, etc., as each of these means a different action on your part. The overall categorization of the issues is useful, but it is even more useful when this information is available for each domain, in order from the most recipients down to the least. Know that AOL is blocking 100% of your email as spam is far more important than knowing 5% of your total email was not delivered because it was mark as spam.

Look through the top domains for signs of problems. A small unknown user rate, or a little greylisting shouldn't be a big concern, but if you see any metric going over 5% it's an indication that you need to change something. If you have a high unknown user rate, you need to look at what has happened with your opt-in process. If it is the first send, a higher rate of unknown users is to be expected, especially if moving from a less reputable ESP. But on an on-going basis, your unknown user rate should be quite consistent, especially across many different domains. If more than 5% of your email is being marked as spam or rejected in other ways, work with your ESP to get this resolved, but consider carefully what you might have done that would have caused recipients to react poorly to that email.

"Sometimes the best sounding marketing plans don't resonate well with customers, and suddenly you have a high complaint rate on a mailing."

Unknown User Rate Over Time

It is important that your unknown user rate remain low at all times, but when it is graphed over time it can help you see if the rate is changing. Unless your website or procedures have changed, the unknown user rate should remain quite constant. If it is going down, you can celebrate, but if it is inching up, you need to look through your opt-in process and try to identify why more bad addresses are being collected.

Complaints Over Time

It is also important that your complaint rate remain low. Look at the rates over time, and try to ascertain if certain mailings spiked changes in the complaint rate. Sometimes the best sounding marketing plans don't resonate well with customers, and suddenly you have a high complaint rate on a mailing. Look at the content, audience, and subject line to figure out what caused the recipients to complain. If you have a good set of demographics for your customers it may be useful to create a segment that shows you the people that complained, then examine their demographics to get more insight.

Transaction Logs

Transaction logs are the details of the "conversation" that occurs during sending. Since email, when it was first created, was designed to be typed directly on screen, including all the header information, the SMTP protocol is one that can be read and understood without too much effort. However, it is something that some experience can help with, so look for your ESP to be able to help interpret any send logs you find confusing. Send logs are the ultimate statement of what occurred during sending, so you should be able to get to these for any recipient-mailing combination to see for yourself what message the receiving mail server returned. Any ESP that cannot or will not provide to you this information should be avoided.

Open and Clikthrough Rates Across Domains

By looking at the open and clickthrough rates by domain, you can sometimes identify domains that are putting more of your email into the bulk folder. If many of the big domains have roughly similar open and clickthrough rates, but one domain is considerably lower, you may conclude that you have not established a good Reputation score with that ISP. Contact your ESP to help determine what can be done about this

ONLINE EMAIL TRENDS

The vast majority of consumer email is sent to a handful of a dozen or so big companies: AOL, Yahoo, Google (Gmail), Microsoft (Hotmail, Live.com, Outlook.com) are the main ones, but there are others. Several of these companies have announced changes in their email clients that may disrupt patterns that we have gotten used to for many years. Both Microsoft and Google have introduced software that can re-prioritize the inbox contents based on user-controlled metrics that override the standard organization schema, which is based on the time the email was received. This may have the effect of lifting one company's emails to the top of the list, while forcing others down, potentially to the point at which they never get seen. In addition, Microsoft has announced that they will process an automatic unsubscribe on behalf of the recipient if their software algorithms decide the recipient is not interested.

While this might seem like a reason for immediate panic, the effects of the programs simply reinforce the trend that has been happening for many years now – sending to unengaged recipients will decrease the likelihood of email being accepted and viewed by the user. The solution remains the same – be sure you are sending to recipients who want your email, make your content interesting, deliver the kind of content you promised when they signed up, and remove recipients that have lost interest. These strategies will ensure that your email marketing program will generate revenue, regardless of the changes implemented by the big ISPs.

Google

In the summer of 2013, Gmail unveiled a new method of organizing email. Email would be sent to one of five tabs (Primary, Social, Promotions, Updates, and Forums). Email sent to you personally would fall under the Primary tab, while promotional email, such

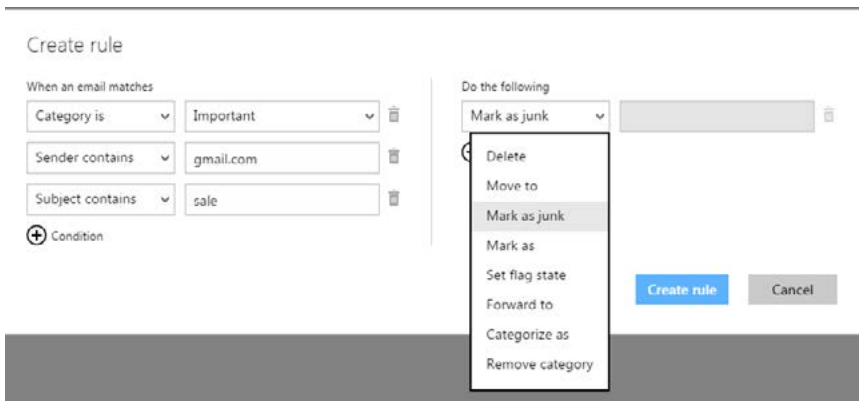
as sale announcements and newsletters would be sent to the Promotional or the Updates folder. This announcement sent the email marketing into a dither. "If all the promotional email ends up in Promotions tab," they argued, "no one will look at it."

Many companies immediately sent out requests for recipients to move their mailings to the Primary folder, thinking this would help their promotions get seen. In fact, nothing could be further from the truth. In the first place, having your promotional mailings sent to the promotional folder is not punishment. That's where it belongs. It's also where most people seem to prefer these sorts of mailings to be. In the second place, no company works harder than Google at foiling those who try to the game the system. Convince someone to move your mailing to the primary folder and the next thing you know your deliverablity might actually drop. For the best results, worry less about whether your mailings end up in the promotions folder, and more about writing engaging subject lines and compelling copy.

At the end of 2013, Google changed the way Gmail worked again, by automatically caching images and switching the default setting to display images. Again, some in the email community announced that the sky was falling, and that the new set-up would play hob with their metrics. Now a year on and the grousing has stopped. While the new set-up has had an effect on certain types of metrics, such as geolocation, it hasn't hurt things over all, and the new display images default has caused an upswing in the apparent number of people viewing promotional mailings in Gmail. In reality, it's doubtful that there was an actual upswing in email views, but the new display default certainly makes it look that way, which helped placate the grumblers.

Microsoft (Outlook.com)

Microsoft has introduced a "Sweep" feature to their email client. First introduced optionally in Hotmail, it is now a regular part of their Outlook.com software. Like Google, it allows users to define rules to "sweep" email into different folders, or even to delete the email automatically, with no opportunity for it to be read. The in May of 2014, they took this idea even further, letting users control what lands in their inbox in a host of way. Now



an Outlook.com user can send the mailings they receive to the junk folder based on any from the age of the email to the words in the subject line. While this does make it easier for the user to categorize their emails however they like, it also has the potential to create situations where innocuous mailings get assigned as spam for no better reason than the use of one word. The list-unsubscribe header is required to send to Outlook.com (Goolara adds this automatically for you), and Microsoft will use this feature to remove recipients that they deem are not interested in your email.

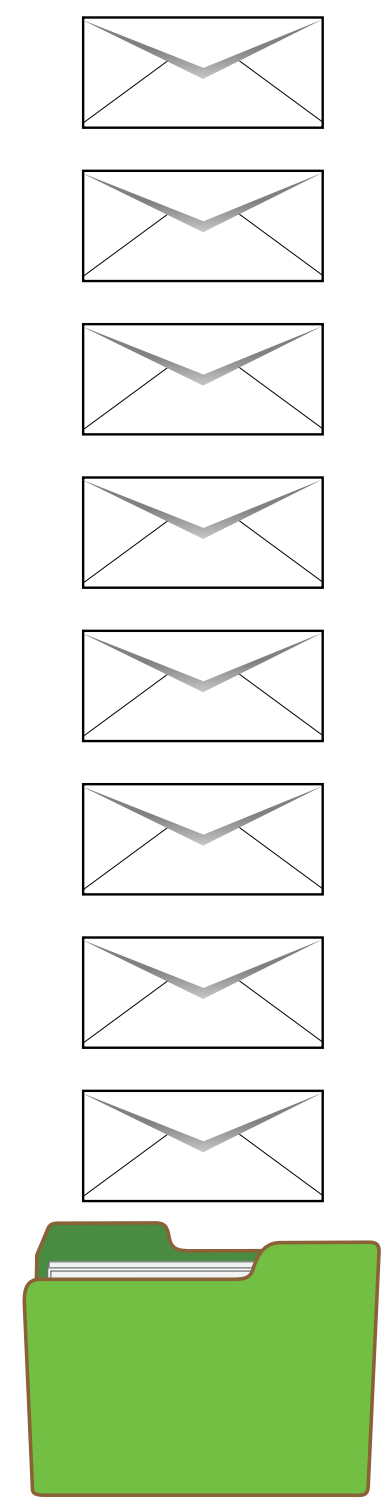
Conclusion

These changes do not make things easier for email marketers, but they also don't change the fundamental fact that to maintain good deliverability you must send to ***engaged*** recipients. These applications could be dangerous if they start automatically and arbitrarily unsubscribing recipients who really do want to receive that email, but there is no evidence of this happening at this time. It is our expectation that there will be some hiccups with these kinds of applications, but the trend toward automatically determining an engagement level for recipients and enforcing it appears to be one that will become more popular over time, not less. As marketers, we must learn to adapt and adjust our approaches accordingly.

SUMMARY

How well your email is delivered is contingent on many things. Reputation Score, send volume, bounce rate, text-to-image ratio and link reputation can all affect deliverability. Some of these factors are more important than others. Your Reputation Score is set by the ISPs and is based on how recipients respond to your mailings. Email that is deleted without opening, or is marked as spam may affect your Reputation score. Keywords and domain blocking are still used by IT departments to block email, even if the email might be something that the recipient wanted to receive.

The best way to ensure good deliverability is to start with good addresses. Although the single opt-in procedure makes it possible to build an email list more quickly, the double opt-in procedure ensures better deliverability. Keeping your recipient list free from unknown addresses is important to good deliverability. Some ISPs may use invalid addresses to monitor unwanted email. Buying lists or appends is not recommended. It often leads to higher complaint rates.



To avoid greylisting issues, good email software will automatically throttle back the sending rates based on the responses from the ISPs. It will also react quickly to unknown addresses before they affect the sender's Reputation Score.

You should not overlook the importance of the sender's identity as it appears in the "Sent From" information. Recipients will often use this information to determine their next step with the email. Generic names, or "Do Not Reply" are

turn-offs to many people and appear to have a slight negative impact on Reputation Scores. You should also keep in mind that not everyone looks at their email on a computer. More and more, people are using their smart phones to check their email.

It is vitally important that you respond immediately to all opt-ins with a welcome message. It is your first opportunity to interact with your potential client. The longer you wait, the more likely they are to forget that they opted-in to receive your email, and may perceive your email as spam.

Good recipient list building requires on-going maintenance. Inevitably, some subscribers will either opt out (unsubscribe), start automatically deleting your mailings, or mark them as spam. When recipients appear to be unengaged but neither unsubscribe nor assign your mail to the junk folder, a win back program might be an effective way to get them re-engaged. There is no "one size fits all" system for re-engagement campaigns. A recipient's individual response to your mailings will determine the best approach for a win-back program if one is warranted at all. The email marketer that keeps their customers engaged will come out on top.

To ensure maximum deliverability, it is important to monitor your results. Good reporting capabilities will help make this job easier. Issues such as specific domain deliverability problems, increases in unknown user rates and complaint increases can be spotted more quickly this way. If you find any anomalies in deliverability, you should contact your ESP immediately.

Online email trends, specifically with Google (Gmail) and Microsoft (Hotmail, Live, and Outlook.com) are toward greater control by the recipient over the delivery characteristics of each email, allowing them user to grade email based on how much they want to receive it. With Gmail, features such as image caching and inbox tabs have changed the way Gmail is received, but it has not hurt either deliverability or engagement. In May of 2014, Outlook.com added the ability for users to modify the delivery parameters for everything from keywords to delivery dates.

GOOLARA DELIVERABILITY SERVICES

Goolara is committed to providing the all the services you need to make your email marketing program successful. Our dedicated team of deliverability experts has years of experience working with ISPs and individual companies to investigate and resolve issues.

Hosted customers get their own, dedicated IP addresses, so that deliverability problems of one customer will not affect another. Goolara creates all the necessary records to authenticate your email with SPF, Sender ID, DomainKeys, and DKIM, and provides the information and assistance necessary to help you get these records put into your DNS server for customized "from" addressing. We manage relations with the different ISPs, blacklist authorities, and anti-spam companies to help you to avoid or resolve issues.

For on-premise customers, Goolara will help you establish all the DNS entries and IP configurations you need to ensure your email is authenticated with the major ISPs. This includes the creation and configuration of SPF, Sender ID, DomainKeys, and DKIM technologies. Once everything is configured correctly, we will monitor your system on a daily basis for deliverability or other issues. If you are not getting all your email delivered, we will work with you and the ISPs, as needed to find a solution. The Goolara deliverability team will contact ISPs on your behalf for issue mitigation, as needed.

If we see problems with your content or other deliverability issues that need addressing, we will notify you immediately and help you resolve the problem to prevent it from damaging your Reputation Score.

About Goolara

Goolara has been in the email marketing business since 2005. Symphonie, Goolara's premiere email marketing solution is available in on-premise and cloud-based, SaaS deployments. The powerful software features many advanced capabilities, such as full-featured dynamic content, transactional and triggered email, and customizable report generation features. It is easy to use and runs from a browser-based interface using Chrome, Firefox, Internet Explorer, or Safari. Goolara is headquartered in Moraga, California and can be found online at www.goolara.com.

Goolara, LLC
1030 Country Club Suite D
Moraga, CA 94556
Telephone: (510) 522-8000
(888) 362-4575
Fax: (510) 522-2457

www.goolara.com