

The Role of DNS, Unsubscribes, and Bounces in Email Deliverability

The Role of DNS

The spam battle is escalating: as ISPs get better at identifying and blocking unsolicited email messages, spammers are trying harder to make it past filters. One of the ways they get around filters is by making their unsolicited spam look like your “ham” (legitimate email). Your mail gets blocked because, in one way or another, your mail looks like spam to your recipients’ ISPs.

How can you ensure your legitimate mail isn’t mistaken for spam? You probably already know that certain words, however innocuous, can be suspect when found in the subject line of an email message (think “teen”, “loan” or “credit”). But what you might not know is that many ISPs may be blocking your mail before they even see the subject line. Why? Because they can’t be sure that you are who you say you are.

Helping ISPs verify your identity therefore is a crucial part of ensuring that your email messages make it to the recipient’s inbox. Your email can get past this first delivery hurdle if you (1) have a *static IP address*, (2) have both forward and reverse DNS set up for your domain name, and (3) have an SPF record.

What is DNS?

DNS stands for Domain Name System, and it’s how computers find each other on the Internet. DNS is like one giant phone book in which you can look up a domain name and find the IP address of the computer to which you’d like to connect.

For example, if you wanted to send email to us here at Lyris, your mail server would perform a DNS lookup to determine where to send it. This DNS lookup lets you send mail to the easily-remembered *recipient@lyris.com*, instead of to *recipient@66.160.177.11*, the IP address to which our mail is currently routed.

The Importance of a Static IP Address

In order to have a complete DNS record, you need to have a static IP address for your email server. Static IP addresses are generally used by web and email servers. Generally speaking, a static IP address is “assigned” to a particular computer, and it stays the same, more or less (hence the “static” part of the term).

A *dynamic* IP address, on the other hand, changes every time the computer connects to a network or the Internet. Dynamic IP addresses are typically used by individual users with dial-up or DSL accounts on personal computers. Such users are not typically sending their email directly to recipients; instead, they’re sending their email to their *ISP’s email server*, which is then responsible for the actual sending and receiving of their email.

Usually, you can’t make a complete DNS record for a dynamic IP address, and they are typically not used for email servers. Some email list management programs like ListManager won’t even function correctly if they are configured with dynamic IP addresses. As well, ISPs typically won’t accept email sent directly from “here today gone tomorrow” email servers using dynamic IPs, since these messages are likely to be from a spammer or a virus-infected computer.

Having a static IP is analogous to having a consistent phone number or physical address: it tells the world you're stable in that location and that you plan on being around in the future.

As deliverability expert Robb Wilson of J.L. Halsey puts it, "you're building a relationship with ISPs, and your relationship is integrally linked to that IP address. A lot of companies think that they can't afford a static IP address, but that's not true at all anymore. They're very affordable these days."

DNS, Backwards and Forwards

Because DNS is such an important way of establishing identity on the Internet, spammers will often forge domain names or IP addresses to hide where their mail is coming from. To detect these forgeries, ISPs often perform what's called a *reverse DNS lookup* on incoming messages.

A *forward DNS lookup* begins with the domain name, and checks to see which IP addresses are associated with it. A reverse DNS lookup takes the IP address that's trying to make the connection, and checks to see if there is a registered domain associated with it.

For example, if an incoming message claims to be coming from the *66.160.177.11 IP address*, an ISP would look up the domain to see if it resolves to *lyris.com*. If it doesn't, the message may be a forgery, or the hapless sender may not have a correct DNS entry. In either case, the message will most likely be identified as spam (when ISPs block spam, they shoot first and ask questions later—if at all).

You can help ISPs verify your identity by making sure that your DNS entry is complete and correct. To make sure your domain has all the correct entries, you can use a web site like <http://www.dnsreport.com/>. If you have any questions about the entries there, the person or organization responsible for your domain should be able to answer them and make any necessary adjustments.

So, Where Does SPF Come In?

A newer form of authenticating incoming email is SPF, or Sender Permitted Framework, which was created to help prevent spammers from damaging the reputations of reliable publishers.

In a nutshell, SPF is a more specific DNS entry that lists which IP addresses are approved to send mail for your domain. If a connection comes from a different IP address than that specified in the record, the recipient may rightly suspect a forgery and reject the message as spam. To learn more about SPF, or to learn how to make an SPF record for your domain, see <http://spf.pobox.com/>.

SPF has not been universally adopted, and not all ISPs check for it. But of the many systems proposed to prevent forgeries, it's the most widespread and the most easily implemented.

And Finally

Performing these types of DNS lookups is an easy way for ISPs to differentiate legitimate email publishers from those who are out to scam their customers. Correcting DNS issues won't guarantee that your email gets delivered, but it's a kind of hand-raising gesture that identifies you as a conscientious Internet citizen and displays a willingness to be checked out by the organizations that process your messages. By using a static IP address, having both forward and reverse DNS set up for your domain name and adding SPF information to your record, you're letting the ISPs know that you're one of the "good guys," which makes it far less likely that your email will be mistaken for spam.

Why Unsubscribes Can Be a Good Thing

Can unsubscribes be good? No sender ever wants to lose an address of course, but when one turns bad or a recipient asks to stop receiving mail, it can actually be a blessing in disguise.

Why? Because spammers work hard to make their mail look as legitimate as possible—in other words, to make it look like your mail. So aside from what you send, recipients and ISPs also recognize you as a good sender by how you behave. A clear, easy, and effective unsubscribe process is the perfect opportunity to distinguish yourself as one of the good guys, and this can really help if blockages or other delivery problems should arise.

Here are three more reasons to smile as you're removing email addresses from your list:

1. Unsubscribe requests keep your list vital and responsive

One of the strongest tenets of the federal CAN-SPAM law (http://www.lyris.com/resources/antispam/canspam_faq.html) requires senders to honor all unsubscribe requests within ten days, and the Federal Trade Commission has proposed that the number of days be reduced to three.

Rather than view this new development as a stricture, however, consider that this requirement is actually likely to work in favor of most marketing goals. By processing unsubscribe requests quickly, lists are kept populated with recipients who actually want to receive your mail—and traditional direct marketing wisdom tells us that such recipients tend to be the most interested and responsive to offers and other messages.

So while there's no doubt sending environment is becoming more regulated, the legitimate email marketer should greet unsubscribe requests gladly and view them just as a gardener does pruning: as an opportunity to keep your list well-formed and fruitful.

2. Removing bad addresses has long-term deliverability benefits

Some marketers have a hard time saying goodbye to bad addresses, rationalizing that there's no harm in trying to send to truly undeliverable addresses if there's a chance of getting through.

But this strategy can actually do a great deal of harm to your overall deliverability. ISPs quickly lose patience with senders who repeatedly send to inactive addresses since processing erroneous mail uses their resources. In addition, sending to a high percentage of "dead" addresses can be interpreted by the ISP as an indication that your list may have been harvested and that you—the sender—are a spammer.

So if an address bounces twice, sacrifice it to the cause of greater deliverability and overall ISP relations. Set your software or service to remove it automatically after a couple of failures—and don't look back.

3. Unsubscribes are infinitely preferable to the other way recipients can ask to stop receiving your mail

When recipients ask you to remove them from your list, it means that they're choosing to follow your unsubscribe process, instead of complaining to their ISP that your mail is spam. In this sense, unsubscribe requests are a sign from recipients that they trust you to honor their requests. If there's no easy way for them to unsubscribe, or if past unsubscribe requests have been ignored or failed, they're much more likely to hit the "this is spam" button.

When a recipient unsubscribes from your list, remember that you're simply losing a single email address. On the other hand, when enough recipients click the "this is spam" button, your mail could ultimately be blocked by ISPs, or worse—you could be added to blacklists.

Bounce Basics

When No News is Bad News

Your email could be blocked—and you don't even know it. Even the best successful delivery statistics can hide deliverability problems.

There are of course many legitimate reasons why email messages can't be sent. People switch jobs or change ISPs and don't bother to update their email address with everyone. But to really know why individual recipients aren't getting your mail, you'll need to look at the rejection messages—the bounces.

Bounce Basics

A failed delivery is commonly called a bounce, because the undeliverable message “bounces” back to the sender.

A “soft” bounce is typically due to a transient problem—the recipient's mailbox is full, for example, or the recipient mail server is too busy.

Just because a bounce is soft doesn't mean that repeated attempts to send to the address will be successful. No matter how many times a sender tries, a message will never be deliverable to bob@aol.cmo. Even if the address is legitimate, the recipient may have abandoned the email account so that the mailbox is perpetually full.

A “hard” bounce is generally the result of a permanent problem, for example when the recipient address doesn't exist. In that case, you'll see an error like this:

```
550 Requested action not taken: mailbox unavailable
550 JOHNB@EXAMPLE.COM is not a valid user
```

Hard bounces tell your mail server to stop trying to send to this address.

When a Bounce is a Block

Spam is a scourge not just because it wastes time having to delete it from your inbox, but because it uses your ISP's network resources. A mail server that is busy processing spam has less capacity to handle email people want to receive. It may seem like spam is free, but there is in fact a cost—unfortunately, that cost is largely borne by the recipient.

The usual tactics ISPs and organizations have taken to combat spam is to block suspect messages or senders as soon as possible so as to keep their resources free for legitimate mail. In accordance with the “rules” of the Internet, they are supposed to inform the sender of the reason why the mail was refused.

So a “soft” bounce may be the result of the receiving mail server refusing the connection, either because it's in general too busy or because the connecting mail server is considered to be spamming. These refusals look something like this:

```
Server example.com is not accepting connections
Connection refused by: example.com
```

Sometimes if your server is being “temporarily” blocked, the message will be categorized as a “soft” bounce too:

```
421 anti-spam.example.com has refused your connection as your mail
server has been temporarily blacklisted
```

Many ISPs use “hard” bounces to reject messages they consider to be spam. Here’s an example of that kind of message:

```
550 Blocked for abuse. Please contact the administrator of your ISP or
sending mail service
554 Transaction Failed Listed in deny list
```

While delivery failures are unfortunate, they help you save time and resources because they let you prune the deadwood from your list and keep it full of active, interested recipients. Messages that say your mail is being blocked as spam, while aggravating, are also helpful. If someone at a blacklist or at an ISP sees your mail as a problem, it’s good to know about it so you can contact them and resolve it.

There’s a bigger problem than knowing you’re being blocked—it’s *not* knowing. More and more, the same transactional messages that should be legitimately used to tell you that a recipient no longer exists are being used to reduce spam.

If a domain with previously high deliverability rates suddenly shows a large number of non-existent users, it may be that there’s been a lot of turnover—or it could be that you’re seen as a spammer and they’re trying to make you go away.

The idea is that spammers may not stop trying to send mail to an address if they’re being blocked—they’ll just go to another ISP or change their content so they can slip through. But if they receive a message that a recipient no longer exists, they’ll be tricked into taking that address off the list regardless of where they go.

It’s hard to know how effective this tactic is against spammers; do they really remove inactive addresses? But it can be very “effective” against conscientious senders who unwittingly remove these addresses.

If there is a sudden increase in dead addresses at a particular domain, it could be that there have been massive layoffs—or that your mail isn’t welcome anymore. See if the same people are undeliverable several times in a row, or if they are still undeliverable if you change the format of your mail—plain text instead of HTML, for example.

The “Quiet” Bounce

Success at reaching all the addresses on your list is the ultimate goal. But reaching that goal doesn’t mean your worries are over.

A hundred percent success delivering to a domain without any delivery failures may mean every address at that domain is still alive and kicking, or it could mean that the ISP has given up. Instead of giving useful (or even deceptive) non-delivery notices, it could be just accepting all of your mail, and then dumping it in a bulk folder--or simply deleting it, without forwarding it to the recipients at all.

If a domain has more than a hundred addresses, you should see some failed deliveries from time to time. If you don’t, check and see if there are any actions from recipients at the domain in question. Are there any opens or clickthroughs at all? If not, it’s probable the mail isn’t getting through.

Take Action!

Once you know that your mail is being blocked, you can take action to ensure that it gets delivered.

- Change the format. If you’re sending in HTML, try sending plain-text.
- Slow your sending speed. It’s possible that you’re sending too quickly for the recipient mail server to respond.
- Email the technical contacts for that domain. Show that you are responsible and ethical, and they are likely to let your mail through. They may have suggestions on how to improve your email practices as well.
- Enlist the help of your recipients. If the technical contacts for a domain are unresponsive to you, they’ll probably listen to complaints coming from their customers.

There's one action you absolutely *shouldn't* take: change your sending IP address or domain in an attempt to trick ISPs into thinking that you are a different sender.

It's tempting if your IP address is being blocked to simply change to another one that isn't being blocked. But that's exactly what spammers do. No matter where you go, your reputation will follow you. If your reputation is good, ISPs will be happy to work with you to ensure your mail gets delivered.

Summary

Overall, there are big benefits to getting the dead weight—bad and unsubscribing addresses—off your lists as soon as possible. Long-term deliverability stays high, while your lists stay clean and responsive. Make sure that your email marketing solution is capable of processing bounces and unsubscribe requests immediately and automatically, and then set it up to do so. Not only will your lists stay lively and active, but as a practice, it identifies you as one of the good guys—a responsible sender—and keeps you in good standing with the ISPs, the law, and your recipients.

Take
Control
of Your
Email
Marketing

Founded in 1994, Lyris Technologies provides advanced software and services for email marketing and email delivery. Lyris' solutions are available as software or as hosted applications and are used by more than 5,000 customers worldwide, from Fortune 500 corporations to fast-growing startups.

LYRIS

Lyris Technologies, Inc
5858 Horton Street, Suite 270
Emeryville, CA 94608

USA and Canada: 800-768-2929
International: +1-510-844-1600
Fax: +1-510-844-1598

email: sales@lyris.com
www.lyris.com