



Optimizing Deliverability of E-mails in JangoMail

This document explains steps you can take and settings you can make in your JangoMail account to maximize the deliverability of your e-mails. It also explains steps that we take to ensure the highest possible delivery rate of our customers' e-mails. With more and more organizations taking steps to combat spam, it is important to understand how spam filters work and how to make sure your legitimate e-mails get through to your recipients.

Steps You Can Take

1. Optimize your Subject line

Don't use all CAPS in the Subject line.

Do not put a \$ sign or an ! point in the Subject line.

Avoid words like "cash", "win", "prize", "free", or "discount".

In general avoid words in your Subject line that if you saw in an e-mail to yourself would make you delete it.

2. Eliminate the 4-digit number in the From E-mail Address

To maximize delivery, turn off the 4-digit number in the From E-mail Address. You can set this in your account under **My Options** → **From E-mail Address**.

Some spam filters look for whether the From E-mail Address ends in numbers. The 4-digit number is an option that is there to provide more detailed reporting, but it isn't necessary.

Additionally, another spam filtering technique is called challenge-response. Challenge-response filters send a reply e-mail back to you asking you to click a link before the e-mail that you sent is delivered to the recipient. This verifies that a human being actually sent the e-mail. After this process, your From E-mail Address is white-listed with the recipient, so that future e-mails sent to that recipient won't generate a "challenge". Turning the 4-digit number off ensures that the same From E-mail address is used on all of your outbound mass e-mails, so that you don't have to keep responding to the challenges sent by the same recipients. Therefore, if you prioritize deliverability over reporting, then turn the 4-digit number off.

3. Turn open-tracking off (also known as read-tracking)

Turn off read-tracking. Some spam filters block e-mails if they contain a "web bug". A web bug is the invisible unique image JangoMail places at the bottom of HTML e-mails to provide our customers with open-tracking reporting capabilities. If this particular Reporting metric isn't too important to you, send your e-mails without open-tracking.

4. Send HTML and plain text together, instead of just HTML

If you're sending HTML messages, make sure to also include a plain text alternative for those e-mail readers that support HTML. The reason for this is because spam filters will flag a message as spam if it contains an HTML message but no plain text alternative.

5. Use the JangoMail "Spam Check" Feature

Before you click the "Send E-mail" button in JangoMail, it is recommended that you click the "Spam Check" button. The JangoMail Spam Content Checker uses the SpamAssassin engine to "score" an e-mail for spam content. SpamAssassin is the world's most popular spam filtering software, and it performs over 1,200 tests on an e-mail message. For each test that an e-mail fails, a score is assigned. If the total score is above a certain threshold (usually 5 points), then SpamAssassin classifies the message as spam, and we recommend you make adjustments to your e-mail to get the total score under 5 before you send it out to all of your recipients.

6. In HTML e-mails, use a word or phrase, rather than a URL, as your hyperlink display text

Phishing scams are e-mails sent to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

Some e-mail clients come equipped with a phishing scam detector. Most phishing detectors work by looking for a hyperlink within the HTML portion of the e-mail where the link display text is an actual URL, but is a different URL than from the hyperlinked URL. When using click-tracking, JangoMail modifies the destination URL, so it is important to use a word or phrase as the display text rather than a URL, since the display URL will not match the hyperlinked URL.

For example:

```
<a href="http://jngo.net/y.z?l=www.amazon.com">Click here to go to Amazon.com.</a>
```

is okay, but

```
<a href="http://jngo.net/y.z?l=www.amazon.com">http://www.amazon.com</a>
```

would be interpreted as a phishing scam.

Steps We Take

1. Participation in whitelist programs

JangoMail currently participates in several whitelist programs which helps ensure our customers' e-mails are delivered to their recipients' in-boxes. JangoMail has whitelisting agreements with AOL, Juno/Netzero, AT&T Broadband, Comcast, and participates in third-party whitelisting programs such as [Ironport's Bonded Sender](#) program.

2. Staying off e-mail blacklists

A controversial, yet still widely used method of spam filtering is subscribing to one or more publicly available e-mail blacklists. Blacklists contain IP addresses of companies that are known to have a record of spamming.

JangoMail and its e-mail servers are not blacklisted anywhere, and we take proactive measures to ensure that we maintain an excellent reputation with blacklist operators.

3. Publishing Sender Policy Framework (SPF) Records

JangoMail publishes Sender Policy Framework (SPF) records for not only the domain jangomail.com, but for the domains we host on behalf of our customers. SPF is an open standard that fights e-mail address forgery and makes it easier to identify spam, worms, and viruses via records in the Internet Domain Name System (DNS). Customers using their own branded domains in the From Line of their outbound e-mails are encouraged to publish SPF records within their own DNS servers. JangoMail's support team is available to assist in the composition of the appropriate SPF records. For more information on SPF, please see <http://spf.pobox.com>.

4. Signing e-mail campaigns with DomainKeys/DKIM

JangoMail signs all e-mail campaigns using a jangomail.com From Address with DomainKeys and DomainKeys Identified Mail (DKIM), to ensure optimal deliverability to receivers that authenticate messages based on these technologies, like Yahoo! Mail and GMail. Additionally, JangoMail provides the tools to and instructions for you to set up DomainKeys/DKIM for your own domain if you do not use a jangomail.com From Address. For more information, see the document: [DomainKeys and DKIM Signing with JangoMail](#)

5. Responding to each spam complaint individually

Even though our customers send legitimate e-mails that conform to our anti-spam policies, that doesn't mean that recipients don't complain. Sometimes a recipient may forget that they signed up for a particular list. Therefore, all spam complaints that are reported to us are responded to individually. We begin with an inquiry to the customer as to how the address in question ended up on the list. After obtaining the relevant information from our customer, we compose a response to the complainant and carbon-copy our customer. Often times, after this process, we will receive an apology from the complainant. This ensures that we maintain an honest, clean, and high-integrity relationship with the Internet community at large.

6. E-mail server log file monitoring

A special log file analyzer is used to monitor our e-mail server log files for failed deliveries. This analyzer generates a daily report to our network administrators, who can then determine if there are any domains rejecting e-mail from JangoMail. Sometimes domains inadvertently block e-mail from networks that generate too high a volume of e-mail, even when the e-mail isn't spam. Because we proactively monitor our log files for these types of blocks, we react almost instantly by contacting the appropriate e-mail administrator to remove the block.

7. 24-hour monitoring of our network and our customers

JangoMail administrators proactively monitor the system 24 hours/day to ensure smooth delivery of our customers' e-mails to their recipients. We are also alerted if a customer engages in spamming or sends content that could trigger spam filters on the recipients' side.