Sending Best Practices

Return Path, Inc.

Table of Contents

Top factors that impact sending reputation and deliverability

- Complaints: Ensure all IP addresses and domains are signed up with all available complaint feedback loops. Suppress complainers from your email list.
- Unknown Users: Suppress unknown users after one bounce.
- Spam Traps: Ensure you have a good list acquisition and list hygiene strategy in place. Use opt-in permission methods. Suppress subscribers that are old and inactive.
- Engagement: Strive to give subscribers relevant content when they want to receive it. Highly engaged subscribers increase the likelihood that email will be sent to the inbox.

Authentication

- Implement an SPF record for your domain: SPF identifies which mail servers are authorized to send email from your domain.
    - Openspf.org provides the information to understand and create an SPF record.
    - SPFWizard.net provides a wizard for generating SPF records.
    - For domains not sending email, create an empty SPF record to indicate the domain does not send email (i.e. "v=spf1 –all").
    - Keep the length of the SPF record under 255 characters. The maximum length for a DNS TXT record is 255 characters.
    - Ensure the SPF record does not have more than 10 DNS lookups (include, a, mx, exists, redirect). Include mechanisms may point to other SPF records with include mechanisms which all account against the maximum of 10 lookups. IP numbers do not require a DNS lookup. Exceeding 10 lookups will cause a failure at many.
    - Do not use the PTR mechanism per RFC 7208.
    - The –all qualifier is preferred but ~all is acceptable. Do not use +all or ?all qualifiers as they essentially make the SPF record useless.
    - Use CIDR notation for IP ranges in the SPF record if applicable (e.g. "v=spf1 ip4:192.168.0.1/16 –all"; which allows any IP address between 192.168.0.1 and 192.168.255.255).
    - Keep the SPF record up to date. Changing service providers and sending from new IP addresses can cause SPF records to be incomplete.
    - Sign outbound email with Domain Keys Identified Mail (DKIM): DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication.
    - DKIM.org provides the information needed to understand and create a DKIM record.
    - Use a key length of at least 1024 bits.
    - Use DKIM instead of DomainKeys. DKIM is an enhanced version of DomainKeys.

o   The "t=y" declaration is for testing and should be removed prior to full DKIM implementation. Some mailbox providers may ignore the DKIM signature while it is in test mode.

o   Rotate DKIM keys at least twice per year to help reduce the risk of being compromised.

o   Create a DMARC record for your domain: DMARC helps ensure that legitimate email is properly authenticating against established DKIM and SPF standards and that fraudulent activity appearing to come from domains under a brand's control is blocked.

o   DMARC.org provides information needed to understand and create a DMARC record.

o   Set the policy (p=) to p=none to get reports when DMARC is first created. If the policy is set it to p=reject before analyzing the reports, the sender will likely encounter deliverability problems. Only change the policy to 'quarantine' and 'reject' once experience is gained from understanding the effects to your email program.

Address collection

- Your address collection process should reject malformed addresses (i.e. me@hotmaiil.com).
- Your address collection process should reject abuse@ and postmaster@ addresses.
- Your address collection should reject role accounts (i.e. sales@company.com, customerservice@company.com).
- Sending a Welcome or Confirmation message from a separate IP space allows for bounce processing of invalid addresses and ensures that high unknown user rates for new subscribers do not impact performance of your regular email campaigns.
- Sending Forward to a Friend messages from a separate IP space ensures that unknown user rates do not impact the performance of your regular email campaigns.

Partner vetting and auditing

It is a best practice to acquire email addresses organically, however, if you receive subscriptions from third party partners, affiliates, or list services:

- Test a sample of the subscription file from a separate IP space and monitor complaint rates, unknown user rates and spam trap hits before adding the file to your database.
- Regularly audit your partner's sign-up process to ensure that it meets industry best practices with regard to address collection.

     returnpath.com

R Return Path

Bounce handling

- Establish hard and soft bounce rules appropriate to your sending practices. It is recommended to suppress unknown users after one bounce.
- Ensure that bounces are appropriately categorized for processing as hard and soft bounces.
- If internal reporting is available, monitor unknown user rates by campaign, by data source, and by sending IP.

Content and conversion

- Send a welcome message series, starting immediately or no later than 24 hours after sign-up.
- Provide content that is consistent and relevant to the expectations set at sign-up.
- Monitor frequency of email to ensure that it is consistent with expectations set at sign-up.
- Brand messages so that the recipient associates it with their subscription to your service. Use an easily recognizable "friendly-from" address.
- If you send multiple types of mail, use consistent branding across messages.
- Test content to ensure that the preview pane is appealing and appropriately identifies your company.
- Make your subject lines relevant and engaging.
- Make your content skimmable and easy to read.
- Clearly display your calls-to-action throughout the message, including the top of the message.
- Ensure your content and calls-to-action can be understood with images disabled.
- Use responsive design to optimize viewing on all email clients, but especially for mobile email clients.
- Include a brief, interesting, and clickable pre-header summary that differs from your subject line and primary headline.

Engagement and retention

- Send targeted email: Capitalize on local events, weather patterns/forecasts, flu/cold outbreaks, etc.
- Use personalization as a means to connect with your customer.
- Have a regular testing strategy for subject lines, content, and frequency to determine what leads to higher engagement rates.
- Optimize transactional messages to keep your customers informed as well as to subtly promote other products or services that may interest them. Be careful not to make other product or service promotions the primary focus of the message.

 returnpath.com

Unsubscribe processing

- Your unsubscribe process should reject requests for malformed addresses (i.e. me@hotmaiil.com).
- Your unsubscribe process should reject requests for addresses that are not in your database.
- Include instructions for unsubscribing in every applicable email.
- Provide any easy to use method for unsubscribing. Ideally, the request is made with "one-click". Do not require a login and a password to unsubscribe.
- Provide multiple venues for subscribers to unsubscribe, including replying to the email and preference centers.
- Provide a website confirmation of the address requesting to be unsubscribed. Set expectations about the time frame required to process the request.
- Process requests to unsubscribe as quickly as possible, and ideally before the next email campaign is sent.

Database maintenance and list hygiene

- Establish an on-going process for actively removing subscribers that are both old and inactive. This will help reduce the likelihood of sending to spam traps.
- Have a plan for non-responders. Identify when subscribers dis-engage and send them messages to win-back their business.
- Send occasional surveys to get additional feedback about how to improve.
- Implement a companywide suppression list and do not send to subscribers on the suppression list unless the subscriber opts-in again.

 returnpath.com