Email Deliverability in Pardot

Salesforce, Winter '22

'22

CONTENTS

EMAIL DELIVERABILITY IN PARDOT

In email marketing, there's a lot that happens behind the scenes after you send an email and before it actually arrives in a recipient's inbox. To make sure emails reach your audience, it's important to understand how email delivery works and practice good deliverability habits. Use this guide to help you better understand email deliverability, troubleshoot delivery issues, and learn best practices for deliverability in Pardot.

> **Note:** Pardot offers tools to help you meet your email marketing goals, but you're responsible for your sending reputation and deliverability. There's no tool that can help deliverability if you're not following best practices.

How Email Sending Works
When you send an email, it undergoes a series of checks and transfers before it reaches your subscribers. A sent email isn't considered successfully delivered until it reaches the recipient's inbox.

Definitions
Review some key deliverability terms we use throughout this guide.

Best Practices for Email Deliverability
Let's review best practices for email deliverability.

Monitor Deliverability
Keep an eye on how your emails are performing using Pardot's reporting tools so you can adjust your email marketing strategies accordingly. For additional insight, contact Pardot support to request a reputation audit.

Get Help
Pardot can't control your sending reputation or guarantee the delivery of your emails. However, we can help you understand how to manage your deliverability and answer any questions you have. If regular Pardot support isn't able to help, we have a dedicated team of delivery specialists to assist you.

Common Deliverability Issues and Questions
Troubleshoot and find answers to the most common issues and questions around email deliverability.

How Email Sending Works

When you send an email, it undergoes a series of checks and transfers before it reaches your subscribers. A sent email isn't considered successfully delivered until it reaches the recipient's inbox.

After you click send, Pardot validates your email, ensures merge fields or variable tags are properly formatted, and rewrites any trackable links. Then, Pardot transfers the email from our outgoing server to the recipient's email server, such as Gmail or Outlook. At this point, the email is sent but not delivered.

EDITIONS

Available in: All Pardot Editions

Sent	Delivered
The email has gone through Pardot's sending process and is transferred over to the receiving email server	The receiving email server deems the email successful and places it in the recipient's inbox

After Pardot passes the email to the receiving server, we no longer have any control over how it's treated or whether it's ultimately delivered. The receiving server conducts checks to validate the email before it's delivered to the recipient's inbox. Pardot provides the results of the delivery attempt in your email's report. For example, if the email is successfully delivered, you can review opens and click-through rate. If delivery is unsuccessful, you can see spam complaints or the reason for a soft or hard bounce.

Definitions

Review some key deliverability terms we use throughout this guide.

Deliverability
An industry term that refers to the likelihood of an email reaching subscriber inboxes. High deliverability means an email is unlikely to be sent to junk mail or blocked by spam filters.

Spam
Spam refers to irrelevant, inappropriate, or unsolicited messages often sent to a large group of people. Sending spam is against Pardot's permission-based email marketing policy.

Sender Reputation
How you're perceived by internet service providers (ISPs). Your sender reputation is impacted by things like spam complaints and how often your emails are opened by subscribers.

Authentication
Authentication refers to protocols internet service providers (ISPs) use to verify an email is legitimate and not spam. There are a few different types of email authentication that we go over that in the Best Practices section of this guide.

SEE ALSO:

Email Reputation and Deliverability Glossary

Best Practices for Email Deliverability

Let's review best practices for email deliverability.

<div style="float:right">

EDITIONS

Available in: All Pardot Editions

</div>

Get Permission
Pardot's permission-based email marketing policy states that you can only send to prospects who have expressly opted in to receive marketing emails from you. Permission-based email marketing is a baseline best practice and it's vital to achieving good deliverability. Use tools like Pardot forms and landing pages to allow prospects to opt in to marketing emails. You can also set up custom email preference center pages to allow prospects to manage their list subscriptions.

Keep Prospects Engaged
The best thing you can do for your deliverability is maintain a permission-based list of engaged subscribers. Engagement means subscribers are actively opening and clicking your emails. Internet service providers (ISPs) monitor for activity, so if your marketing emails are consistently left unopened, they start treating them as spam.

Send Quality Email Content
Content consists of your email's subject and body. Some spam filters evaluate email content when determining whether a message is spam. Here are some best practices to keep your legitimate emails from triggering spam filters.

Use Email Authentication

With Pardot, you can send emails from your domain by authenticating through the two most widely accepted email authentication standards: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). Major ISPs and corporate spam filters check for one or more of these types of authentication when determining whether to allow emails to a recipient's inbox. Setting up email authentication is critical for achieving good deliverability.

Use a Dedicated Sending IP Address

A dedicated sending IP address gives you full control of your email sending, so you're fully responsible for the reputation of your own IP address. A dedicated IP service is best for clients sending a consistently high volume of emails. In Pardot, you're considered a high-volume sender if you regularly send more than 100,000 emails per month. Shared IP addresses are best for lower-volume or inconsistent senders.

Get Permission

Pardot's permission-based email marketing policy states that you can only send to prospects who have expressly opted in to receive marketing emails from you. Permission-based email marketing is a baseline best practice and it's vital to achieving good deliverability. Use tools like Pardot forms and landing pages to allow prospects to opt in to marketing emails. You can also set up custom email preference center pages to allow prospects to manage their list subscriptions.

SEE ALSO:

Create a Custom Email Preference Center Page

Set Up a Confirmed Opt-In Process

Pardot's Permission-Based Email Marketing Policy

Keep Prospects Engaged

The best thing you can do for your deliverability is maintain a permission-based list of engaged subscribers. Engagement means subscribers are actively opening and clicking your emails. Internet service providers (ISPs) monitor for activity, so if your marketing emails are consistently left unopened, they start treating them as spam.

Pardot includes tools to help you identify and suppress unengaged prospects who could harm your sending reputation.

Create a Dynamic Suppression List

To prevent your customers from experiencing marketing fatigue, space out the timing of your emails with a suppression list. Create a dynamic list with a rule type that filters based on the recency and frequency of email sends.

Identify and Suppress Unengaged Prospects

Keep your deliverability high by practicing good list management and not emailing unengaged prospects. Use a dynamic list to suppress an unengaged prospect from receiving Pardot emails.

Create a Dynamic Suppression List

To prevent your customers from experiencing marketing fatigue, space out the timing of your emails with a suppression list. Create a dynamic list with a rule type that filters based on the recency and frequency of email sends.

During the setup for a dynamic list, you choose which rules to match prospects against. To use the dynamic list as a suppression list, select the **Prospect has been emailed** rule. Enter the number

> EDITIONS
>
> Available in: All Pardot Editions

of sends and the time frame, and run the rule. Include the dynamic suppression list when you send marketing emails and to remove prospects who meet the criteria you set.

Keep these considerations in mind when you use the Prospect Has Been Emailed rule.

- The rule considers list emails and email sent from Engagement Studio only.
- We recommend that you wait about 10 minutes between email sends. Allow time for the system to process an email send and mark a prospect accurately.
- A day is the time between 12 AM and 11:59 PM in the user's time zone.
- When you use the suppression list in an engagement program, suppressed prospects pause at the step they're on. When the time period is up, they resume the program and start receiving the paused emails.
- If your account has multiple prospects with the same email address, the rule counts all list emails sent to prospects with that email address. For example, Prospect A and Prospect B have the same email address. You sent each prospect two emails in the last three days. The rule type counts four emails sent in the last three days.

Identify and Suppress Unengaged Prospects

Keep your deliverability high by practicing good list management and not emailing unengaged prospects. Use a dynamic list to suppress an unengaged prospect from receiving Pardot emails.

Before you begin, define what an unengaged prospect looks like to your organization. Here are a few ideas to get you started.

- Have you sent 20 daily emails with no prospect activity?
- Have you sent six weekly emails with no prospect activity?
- Have you sent six monthly emails with no prospect activity?

1. Create a list.
2. Select **Dynamic List**.
3. Click **Set Rules**.
4. For Match Type, select **Match All**.
5. Add a rule, and select **Prospect has been emailed**.
6. Enter the time details for the rule.
7. Add a rule, and select **Prospect time**.
   a. From the first dropdown, select **last activity days ago**.
   b. From the second dropdown, select **is greater than**.
   c. Enter the number of days.
8. Save the list.

The list populates with unengaged prospects. Use the list as a suppression list for your email sends. If a prospect becomes active again, they are removed from the list.

Send Quality Email Content

Content consists of your email's subject and body. Some spam filters evaluate email content when determining whether a message is spam. Here are some best practices to keep your legitimate emails from triggering spam filters.

Avoid Interactive Content

Some kinds of interactive content can cause your emails to be marked as spam. Including the following in your email code sometimes triggers spam filters:

- JavaScript
- RSS feeds
- Forms

Keep Your Code Clean

One of the most common causes of sloppy email HTML is copying and pasting from Microsoft Word. When you copy-paste content from Word, it pulls in style tags and other code. If you must copy-paste, use the **Paste From Word** button.

Keep the Image-To-Text Ratio Low

Too many images or too large of an image compared to the amount of text in an HTML email can make your message look spammy to a filter. Adding more text and reducing the number and size of images can help.

Keep in mind that some email clients block images by default, so your recipients don't see the images automatically. Include alt tags that describe your images in case they don't load for the recipient.

Be Careful with Links

Avoid using URL shorteners in your emails. Spammers frequently abuse them, and some shortened domains have been placed on widely used block lists. Many spam filters block emails that contain shortened links from shortened domains.

Most spam filters consider emails with links to several domains spammy, so limit the number of different domains that you link to in an email.

Include the Physical Address and a Way to Opt Out

Marketing emails must contain two things: your physical address and a way for recipients to opt out of future emails. If your marketing emails are missing an unsubscribe or email preference center link or a physical address, they can trigger spam filters. However, Pardot automatically includes an unsubscribe link on your marketing emails, so don't worry about adding this information.

Use Email Authentication

With Pardot, you can send emails from your domain by authenticating through the two most widely accepted email authentication standards: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). Major ISPs and corporate spam filters check for one or more of these types of authentication when determining whether to allow emails to a recipient's inbox. Setting up email authentication is critical for achieving good deliverability.

Sender Policy Framework (SPF)

SPF is a form of email authentication that makes forging the sender of an email, or email spoofing, more difficult. SPF isn't aimed at stopping spammers. Rather, it tightens loopholes used by spammers to spoof emails. SPF provides a list of all outbound email sources for a domain as a DNS TXT record.

When a receiving mail server gets a message appearing to be sent from a certain domain, it checks the sender's SPF statement to verify that information.

DomainKeys Identified Mail (DKIM)

DomainKeys is an email authentication system that verifies the DNS of an email sender and the message's integrity.

Domain-Based Message Authentication, Reporting, and Conformance (DMARC)

A third layer of authentication that's becoming more widely used is domain-based message authentication, reporting, and conformance, or DMARC. With DMARC, you notify receiving servers that your messages use SPF and DKIM and instruct them on what to do if they fail those authentication checks.

Pardot can't set up a DMARC policy for you, but we can help you ensure your emails are DMARC-compliant. For more information, contact Pardot support.

SEE ALSO:

Implement DKIM and SPF Email Authentication

Use a Dedicated Sending IP Address

A dedicated sending IP address gives you full control of your email sending, so you're fully responsible for the reputation of your own IP address. A dedicated IP service is best for clients sending a consistently high volume of emails. In Pardot, you're considered a high-volume sender if you regularly send more than 100,000 emails per month. Shared IP addresses are best for lower-volume or inconsistent senders.

A dedicated sending IP offers some benefits for high-volume senders.

EDITIONS
Available in: Pardot **Advanced** Edition Available for an additional cost in: Pardot **Plus** Edition

- A dedicated IP address gives you more control over your sending reputation. On a shared IP address, you're affected by the sending practices of everyone on the address.

- In industries with heightened security, like banking and defense, a dedicated sending IP address is more likely to be allowlisted than a shared address. When your sending IP address is allowlisted, your emails are more likely to stay out of the spam folder.

Warming a Dedicated IP Address

New IP addresses are considered "cold" until they've established an email sending reputation. Mail servers tend to treat messages that are coming from a cold IP address as spam. IP warming is a process that helps you establish a reputation as a legitimate email sender. It's best to start small and gradually send to larger volumes of prospects. IP warming gives receiving servers time to observe your sending patterns and behavior and builds a solid sending reputation.

Warming a Dedicated IP Address

New IP addresses are considered "cold" until they've established an email sending reputation. Mail servers tend to treat messages that are coming from a cold IP address as spam. IP warming is a process that helps you establish a reputation as a legitimate email sender. It's best to start small and gradually send to larger volumes of prospects. IP warming gives receiving servers time to observe your sending patterns and behavior and builds a solid sending reputation.

Getting Started with a Dedicated IP Address

Before you can start warming your IP address, make sure you take care of these prerequisites.

- To make sure that your users can receive test emails, allowlist your new sending IP on your corporate receiving server.
- Check your SPF statement and make sure you're using **include:aspmx.pardot.com**. You can check your SPF statement by navigating to **Admin** > **Overview**. To view your SPF statement, scroll to Email Sending Domains, and click **Error** or **Verified**. If include:aspmx.pardot.com isn't in this statement, have your IT team update your SPF record.
- Segment out your best and most active contacts. Don't start your IP warming with old lists! Having high delivery rates with your initial campaigns helps build your IP's sending reputation.

Warming the IP Address

The key to warming your IP address is to spread out your email sends over multiple days. For example, if you plan to send 200,000 emails a week, split your lists into 20 sublists . Don't include more than 10,000 recipients in each list. Email only one sublist per day over the first few days. A consistent mail volume day-to-day is better than a large volume spike on one day of the week and no email sent on remaining days of the week.

A good rule for larger ramp-ups is to start with 10,000 prospects per day. If your bounce rate stays below 10% and your spam complaint rate stays below 0.1%, double your sending per day over the next few weeks. Continue this rate until you reach your desired sending volume.

This example shows how to ramp up to sending 200,000 emails a week.

Week	Emails Per Day	Total Per Week
Week 1	10k per day x 4 days	40k
Week 2	20k per day x 5 days	100k
Week 3	40k per day x 5 days	200k
Week 4	50k/day x 4 days	200k

Monitor Deliverability

Keep an eye on how your emails are performing using Pardot's reporting tools so you can adjust your email marketing strategies accordingly. For additional insight, contact Pardot support to request a reputation audit.

There are also third-party tools available on the web where you can check your sender score and find out if you are on any known blocklists. If you do find your IP on a public blocklist, Pardot Support can usually help resolve the issue. If you are on a private blocklist for a specific organization, work directly with that organization's IT team to determine next steps.

SEE ALSO:
Pardot Campaign Reporting
List Email Report

Get Help

Pardot can't control your sending reputation or guarantee the delivery of your emails. However, we can help you understand how to manage your deliverability and answer any questions you have. If regular Pardot support isn't able to help, we have a dedicated team of delivery specialists to assist you.

Contact Pardot support

Common Deliverability Issues and Questions

Troubleshoot and find answers to the most common issues and questions around email deliverability.

Your internal tests are going to spam
When you send an email from your company domain to your company domain, but from an unfamiliar IP address, it can flag spam filters. To avoid this problem, allowlist your Pardot sending IP and remove it from any other spam or security filters you have in place.

Your emails go to spam when sent by Pardot but not by Gmail
Gmail is built for individual, or 1:1 email sends, while Pardot is an email marketing tool. These classifications play a critical role in how email servers consider emails that come from each. To help stop malicious spam, spam filters take a closer look at emails sent through bulk email services like Pardot.

To help prevent your emails from being marked as spam, ask your prospects to allowlist your sending IP, just as you did internally. Add a line of text to your emails that explains what to do if they don't want to miss your emails. For example: "Heads up! Sometimes email providers like Gmail or Yahoo! don't deliver marketing emails because they mistake them for spam. To avoid this, please add [sender email address] to your list of preferred senders."

Locate email bounce codes
Navigate to your email report in Pardot and click the number of soft or hard bounces. Bounce codes are generated by the recipient's email server. Pardot translates the more common bounce codes, but you can find more information with a quick web search.

Confirm that your SPF, DomainKey, and DomainKey Policy entries are correct
In Pardot Classic: **Admin > Domain Management**. In Pardot Lightning App: **Pardot Settings > Domain Management**. If everything is verified and working correctly, the SPF and DomainKey Policy columns shows green checkmarks. If you don't see green checkmarks, confirm setup and functionality by using external sites for SPF and DKIM. If an alternative setup is being used or if a new entry has been added within the last 24 hours, green checkmarks sometimes don't appear.

You can also send a test email to yourself and inspect the email headers to diagnose the problem. A successful email has a PASS value under SPF and DKIM. Depending on your email client, the location of headers and the way they look can be different. If it doesn't pass, make sure you're using your Pardot account's sending IP and the domain matches your Domain Management page.

If the email shows both PASS values, but still goes to spam, contact Pardot Support for further investigation.

EDITIONS

Available in: All Pardot Editions

Your emails are being placed in Gmail's Promotional tab

Pardot doesn't have control over which tab Gmail chooses for your email. Keep in mind, the Promotional tab is still your recipient's inbox. In fact, it can actually reduce the number of spam complaints and opt-outs. When recipients know that they're looking at a marketing email, they're sometimes more likely to react positively.