A Practical Guide for Effective Email Outreach

Introduction

Email outreach is a critical tool for connecting with your target audience, but it comes with challenges. High bounce rates, poor deliverability and low engagement can undermine your outreach efforts, damage your sender reputation and limit your campaign's overall success.

PDL's high-quality email data can help you overcome these challenges by ensuring that you reach the right contacts using accurate, up-to-date information.

In this guide you will learn how to:

1. Select the appropriate PDL email fields for your use case
2. Validate email data to minimize bounce rates
3. Leverage domain warmup strategies to protect your sender reputation
4. Evaluate your performance to ensure strong, ongoing deliverability

By following these best practices, you can enhance your email deliverability, protect your domain health and drive stronger engagement with your outreach campaigns.

---

1. Selecting the Right PDL Email Field

PDL builds comprehensive person records that include both and historical email information to support a variety of use cases. As a result, these records often contain multiple email addresses. To help ensure the success of your outreach campaigns, it is crucial that you

leverage the appropriate email field for your specific purpose[1].

Candidate Outreach

When reaching out to potential job candidates, we recommend using the `recommended_personal_email` field first. This field represents the best available personal email address for contacting candidates directly, helping ensure that your outreach connects with them outside of their work inbox.

To expand your reach, you can also reference the `personal_emails` array, which includes additional personal email addresses associated with the individual. However, we advise starting with the `recommended_personal_email` before using additional emails in this array.

Sales and Marketing Outreach

For business-related outreach, such as running sales or marketing campaigns, we recommend using the `work_email` field. This field contains an individual's current professional email address, helping you reach your contacts within their professional work environment.

It's important to avoid sending outreach to **non-current professional emails**, as outdated work emails can result in high bounce rates and potential compliance risks.

> 💁**What about the `emails` array?**
>
> PDL also provides an `emails` field for each person record, which tracks all the email addresses associated with a person including both historical and current. While this field can be valuable for specific use cases, we **do not recommend using it for outreach purposes**.
>
> The primary use cases for this field are:
>
> - **Matching**: Identifying and matching individuals across different platforms or datasets
> - **Historical Email Analysis**: Understanding email linkage patterns or tracking changes over time
>
> Because this array contains a mix of both historical and current email addresses, using these emails directly in your outreach can lead to problems since many of the emails in this array may be outdated or inactive. As a result, sending outreach to these emails significantly increases the risk of bounces and undeliverable messages, which can harm your sender reputation and domain health.

[1] Please confer with your compliance professionals before using data in a marketing campaign. People Data Labs cannot guarantee all intended uses of data are compliant.

To summarize, **avoid** using the `emails` array directly for outreach. Instead use these fields based on your use case:

- `recommended_personal_email` (and optionally, `personal_emails` if needed) for candidate outreach or use cases where you need to connect via a personal email.
- `work_email` for sales and marketing outreach and other use cases where you need to connect via a professional work email.

---

2. Email Validation

It is important to validate any emails you intend to use in order to ensure their deliverability; this is true whether you are about to kick off outreach or just collecting emails to store for later. Email validation needs to be refreshed regularly because email addresses become inactive or invalid over time. People change jobs, abandon personal emails or switch domains, meaning even your previously validated email addresses can stop working. This is true for any emails you use whether they come from PDL or other providers.

We recommend using a trusted validation service, such as Bouncer.com to regularly verify emails. At a minimum we recommend validating your emails at least once a quarter, but ideally immediately before any large outreach campaigns or anytime you begin to notice large drops in deliverability.

> **Bouncer Email Validation Partnership**
>
> With Bouncer in particular, PDL customers have access to discounted incentives to help minimize the cost of integrating email validation into your outreach workflow.

To summarize, **use an email validation service** like Bouncer.com to validate any emails you intend to use to ensure deliverability and protect your domain health. We recommend validating at least once a quarter as well as **before** kicking off any large outreach efforts.

---

3. IP / Domain Warmup

If you plan to send emails from a new domain or IP address, we strongly recommend implementing a **Domain Warmup** strategy. Domain warmup is the gradual process of increasing email volume over time to build trust with Internet Service Providers (ISPs) and Email Service Providers (ESPs). This standard practice is easy to implement and plays a crucial role in keeping your emails out of spam folders while protecting your overall domain reputation.

For best results, use a dedicated IP rather than a shared IP to ensure you are not inheriting a poor sender reputation. Services like **Outreach** allow you to integrate with **SendGrid**, which

provides dedicated IPs and built-in warming features to automate this process. Additionally, SendGrid simplifies the configuration of essential email authentication records - SPF, DKIM, and DMARC - which help improve deliverability and reduce the likelihood of emails being marked as spam.

Example Domain Warmup Strategy

If you're not using a service like SendGrid, you can structure your domain warmup strategy using a phased approach. Below is an example to help you get started:

Phase 1 (Weeks 1-2): Start Small

- Begin with a low email volume targeting a small group of your most highly engaged recipients (**50-100 emails per day**)
- Focus on individuals who have explicitly expressed interest in your emails, such as **existing customers or recent sign-ups**
- Prioritize **high open and engagement rates** to signal to ISPs and ESPs that your emails are relevant and trustworthy

Phase 2 (Weeks 3-4): Gradually Increase Volume

- After the initial phase, **increase your daily email volume by approximately 50% every 2-3 days**. For example:
  - **Days 1-3**: 50 emails/day
  - **Days 4-6**: 75 emails/day
  - **Days 7-9**: 110 emails/day
- Continue this gradual increase until you reach your desired sending volume
- With each step, continue to prioritize **engaged audiences** to maintain strong performance metrics and a positive sender reputation

There are many ways to extend or customize your domain warmup strategy, but the example above provides a reasonable starting point to cover the basics. The most important concept is to gradually increase your send volume while maintaining high engagement rates. A well-executed warmup strategy can be simple to implement, but is a crucial foundation for developing a positive, long-lasting domain reputation.

SPF, DKIM, and DMARC Records

While implementing your domain warmup strategy, it is essential to configure your SPF, DKIM, and DMARC records correctly. These email authentication protocols help improve deliverability, reduce the risk of spoofing, and enhance your domain's reputation.

SPF (Sender Policy Framework): Ensure your SPF record is correctly set up to specify which IP addresses are authorized to send emails on behalf of your domain. This helps prevent spammers from using your domain to send fraudulent emails.

DKIM (DomainKeys Identified Mail): Set up DKIM to add a digital signature to your emails, confirming their authenticity and integrity. This enhances email security and builds trust with ISPs and ESPs.

DMARC (Domain-based Message Authentication, Reporting & Conformance): Configure DMARC to tell ISPs how to handle emails that fail SPF or DKIM checks (e.g. reject or quarantine them). DMARC also provides you with reporting insights into potential abuse of your domain.

> 📘For details on how to set up and configure these records for your domain, see this guide: How to Set Up Domain Authentication

By ensuring these records are correctly configured, you'll improve the chances of your emails being delivered to recipients' inboxes and avoid being marked as spam.

Maintaining Strong Deliverability

As you continue your email outreach, here are a few key practices to ensure your emails stay out of spam folders and maintain a healthy sender reputation.

1. Test Your Deliverability

To make sure your emails are being successfully delivered, use a tool like GlockApps to regularly test your deliverability. Tools like these allow you to simulate how your emails will be treated by different ISPs and email clients, helping you identify if your emails are landing in spam folders. By catching issues early, you can make the necessary adjustments to improve deliverability and maintain a positive sender reputation.

2. Provide an Opt-Out Mechanism

We strongly recommend always including a clear and easy-to-find opt-out mechanism (i.e. unsubscribe link) in your emails. This not only helps with legal compliance (like GDPR or CAN-SPAM), but also minimizes the risk of recipients marking your emails as spam. It should be no surprise that frequent spam reports can damage your reputation and may likely result in ISPs blocking your ability to send emails altogether.

3. Monitor Your Send Metrics

You should also keep a close eye on key performance metrics to gauge the effectiveness of your email campaigns. Some specific metrics to consider include:

- **Bounce Rates**: High bounce rates may indicate invalid email addresses or deliverability issues.
- **Spam Reports**: If too many recipients mark your emails as spam, it can significantly impact your reputation and future sends.
- **Successful Deliveries**: Track the number of emails successfully reaching recipients' inboxes to ensure your email list is clean and your campaigns are performing well.

By regularly monitoring these metrics, you can quickly address any issues and ensure that your emails continue to reach your intended audience while maintaining a strong and trustworthy sender reputation.

Conclusion

By following the recommendations outlined in this guide, you can optimize your email outreach campaigns to achieve better results.

- **Targeted Outreach:** Use the appropriate email field based on your use case and whether you need personal vs professional emails
- **Email Validation:** Validate all email addresses using a service like Bouncer.com before sending outreach
- **Domain Warmup**: Gradually increase your email volume from new domains or IP addresses to build trust with ISPs and maintain strong deliverability
- **Testing and Monitoring**: Continually test and monitor your email performance to address potential deliverability issues before they impact your sender reputation.

Coupled with PDL's rigorous data quality standards and monthly updates, these strategies reduce the risks of outdated email addresses, enhance engagement, safeguard your domain health, and maximize the impact of your outreach efforts.

Your PDL Solutions Engineering Team 💜