SALES EMAIL DELIVERABILITY GUIDE

11 BEST PRACTICES FOR HITTING THE INBOX *EVERY TIME*

ONESHOT

TABLE OF CONTENTS

INTRODUCTION

Successful email prospecting relies on a lot of things going right.

→ The subject line needs to capture attention

→ The message needs to resonate with the right person at the right time

→ The CTA must be clear and compelling

Many sales pros believe the formula for success stops there.

But this view leaves out a crucial component—the key that powers successful cold emails, unlocks more pipeline from your outreach, and can make or break your prospecting campaigns.

Email deliverability is the silent workhorse behind every successful cold email.

You can do the most in-depth research. Write the most thoughtful message. Include an irresistible offer.

None of it matters if your email goes to spam.

And if your deliverability is poor, that's exactly where most of your cold emails are ending up.

Don't believe me? Take a look at this screenshot of Gautam's (OneShot CEO & Co-Founder) spam folder:
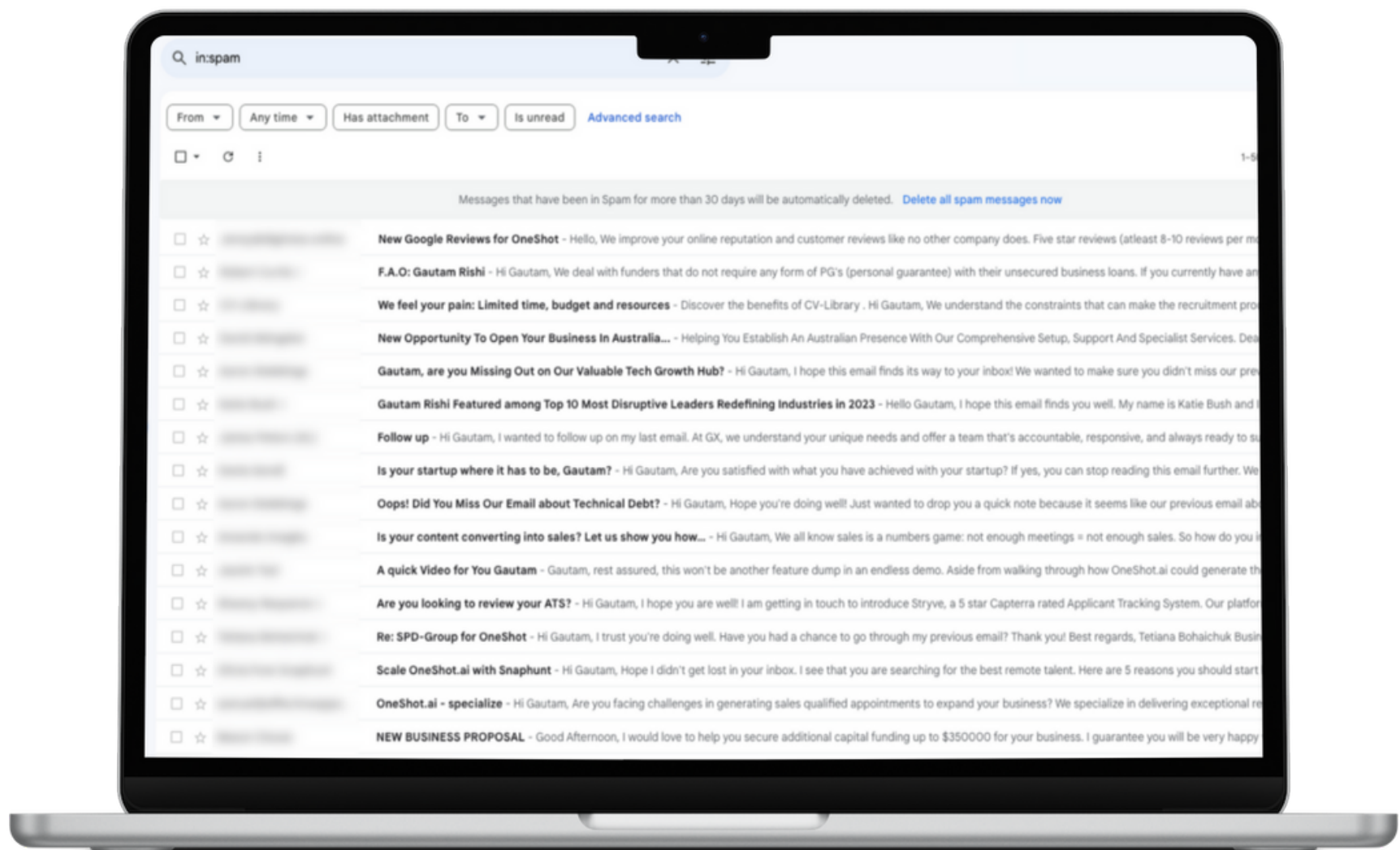
Full of cold emails that went to junk. That's only a couple day's worth.

Email deliverability isn't just IT's problem.

If your sales team relies on cold email to reach prospects, it is <u>very much</u> your problem.

But that's okay. Because problems are made to be solved.

As for email deliverability, while it sounds daunting and technical, there are specific solutions that are quick to implement.

And more importantly, you don't need to be a technical expert to do it.

At OneShot, we've helped dozens of revenue teams fix their deliverability and drive more pipeline with cold email.

Here are our 11 best tips and strategies for fixing yours.

1 ALWAYS PROSPECT THROUGH AN ALTERNATE DOMAIN

If there's one thing you should remember from this guide, it's this:

Never prospect from your primary domain.

Cold emailers are often the primary culprits for email no-nos—think sending lots of emails and racking up too many spam reports. Email clients (Gmail, Outlook, etc.) aren't fans of this behaviour.

When they detect it, they issue penalties at the domain level.

That means each infraction incurred by *anyone* with an email address tied to a particular domain can impact *everyone* at the org and damage the overall reputation of the domain. That means:

→ Everyone at the company will take a deliverability hit, no matter if they're guilty of email sins or not

→ Important emails like investor updates and customer proposals might get sent to spam

→ Organic traffic to your website could be impacted because the domain reputation is slipping

Let's face it. Cold emails, by nature, are unexpected. Some recipients will not appreciate the out-of-the-blue outreach. Spam reports WILL happen.

The best way to ensure these penalties don't impact the ability of your entire company to communicate online is to run your email prospecting campaigns though a separate domain.

Your company probably already owns a bunch of alternate domains similar to your primary. It's a defensibility play. Most of the time they just sit there.

Take one. Use it for your prospecting campaigns.

Set up a couple of accounts under this new domain. The number of cold emails you can safely send goes way up if you get a couple going. This also acts as a sandbox to test and experiment new outreach strategies.

Best part? Your primary domain's reputation & performance remain unaffected.

Important: The alternate domain you use to prospect needs to have the SPF, DKIM and DMARC records properly set up. See tip #3 for more on that.
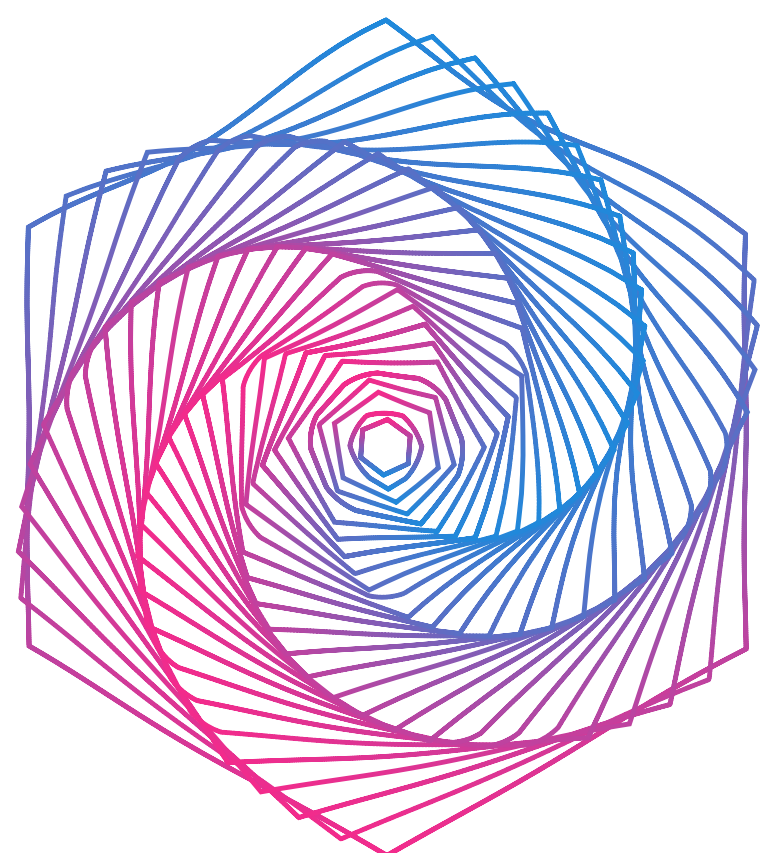
2 ROTATE MAILBOXES

Alongside sending through an alternate domain, it's also a smart practice to rotate through several mailboxes.

One way email clients detect spamming activity is by monitoring the number of emails sent by an account per day.

This strategy allows you to increase the number of emails you can send and also spread the risk of penalties across multiple mailboxes, rather than concentrating it on just one.

Once you set up an alternate prospecting domain, create several accounts or users for each person who will be using it.

For example, if Joe Smith is on my team at Acmecorp, I'll create the following accounts:

- joe@acmecorp.com
- joe.smith@acmecorp.com
- jsmith@acmecorp.com

It's important that these accounts are tied back to a real person on your team. Interested prospects will likely do a search for the person who's emailing them to see if they and their company are legit.

When my prospect searches Joe Smith at Acmecorp on LinkedIn, you'll want to make sure he pops up.

Using different mailboxes can also facilitate A/B testing of your email content, subject lines, and send times. This can provide valuable data to help optimize your cold email campaigns.

3 VERIFY YOUR EMAIL AND YOUR DOMAIN

Authentication proves that an email coming from your domain is legitimate.

When we're talking deliverability and authentication, these are the big 3 protocols:

SPF: Sender Policy Framework (SPF) is like the bouncer for your inbox, checking the ID of the emails trying to come in to make sure whoever's sending them are who they say they are.

DKIM: DomainKeys Identified Mail (DKIM) is an authentication method that checks for a digital signature or key. It confirms the sender is legit and detects forged or altered addresses.

DMARC: Domain-based Message Authentication, Reporting and Conformance (DMARC) is a mouthful the final boss. It provides domain-level protection to prevent unauthorized use and email spoofing.

Email providers will automatically check all this stuff in the microseconds between you hitting send and your email (hopefully) reaching your recipient.

You can check yours for free.

Mail-tester.com and MxToolbox are free tools that will evaluate the health of your email.

They'll check your SPF, DMARC, and DKIM records to make sure you're validated.
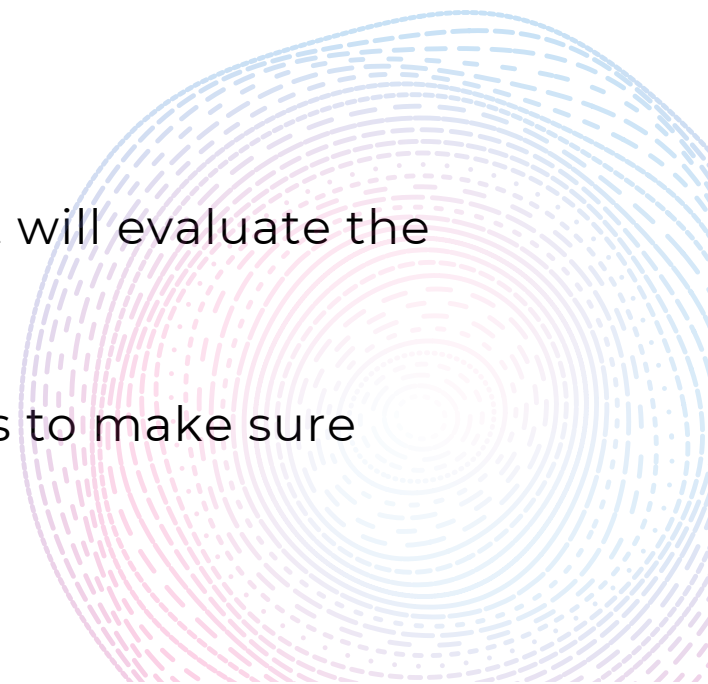
But they're a little light on what to do if one of these parameters isn't scoring well.

To get a detailed report of your email health and actionable tips on fixing any issues, try OneShot's free email health and deliverability tool. You'll be able to see:

- If you're authentication protocols are set up correctly
- Whether you're on any blacklists
- How to fix any potential issues

To grab your report, send an email to checkmyemail@oneshot.ai and we'll reply with a detailed report.

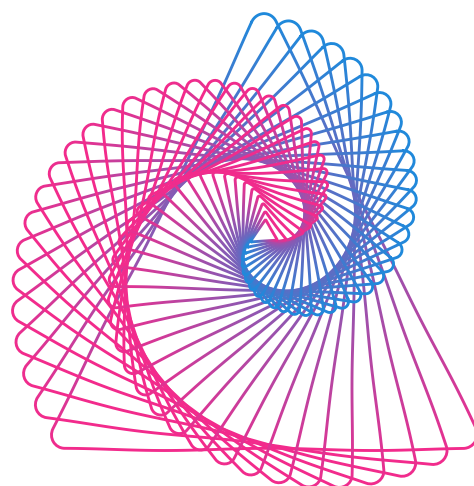# 4 WARM UP MAILBOXES OVER 30 DAYS

One of the gravest mistakes novice prospectors make is setting up a new account and immediately firing off hundreds or thousands of emails.

This approach is sure to land you in spam.

Countless email accounts are opened every day. Email providers are very good at detecting which accounts are being used by real people and which are spamming bots.

Email warming is the process of taking a newly minted email account and "warming it up" by sending signals to email providers that this is a legit account. It's the process of gradually increasing the number of emails sent from a new email address or domain to build a good reputation with email service providers.

There are two main methods for warming up a new email account:

- **Manual warm-up:** Once your new inbox is set up, start emailing teammates, subscribing to newsletters, and responding to emails you receive. This generates natural and authentic engagement signals for your inbox.

- **Use a warm-up tool:** There are tons of tools on the market that will automatically warm up a new inbox for you. The process is the same, but it's usually carried out at a larger scale.

Regardless of the method you chose, it's best to warm up a new account over 30 days to be sure you've provided email providers the right signals for a good sending reputation.

5 MAILBOX THROTTLING

Restricting the volume of emails sent each day is a crucial aspect of maintaining good email deliverability.

Overwhelming email providers with a flood of emails from a single address raises red flags.

When you send too many emails, especially from a new or lesser-known email address, providers may think you're spamming and you could be penalized.

This can lead to emails being directed to spam folders, or even your address being blocked entirely.

A good practice is to send no more than 30 emails per day per mailbox.

This gives you the best chance of keeping your sender reputation intact and your emails landing in your prospect's inboxes.

By combining this limit with the mailbox rotation and alternate domain strategies from above, you can start to ramp up the volume while still staying within those safe sending limits.

Another boon of this strategy is it also helps make sure your reps are intentional about what they send and who they send it to. With a limit to how many emails they can send a day, they can be more thoughtful in their outreach and spend more time researching and personalizing their messages.

Better 30 hyper-personalized, thoughtful messages that land in someone's inbox than 300 generic, identical emails that are probably going to spam.

6 REMOVE SPAM TRIGGER WORDS FROM YOUR EMAILS

Email providers flag certain words they identify as fraudulent or malicious.

They're built to identify terms that typically overpromise or artificially inflate a positive outcome to coax readers into forking over sensitive information. Terms like "buy," "double your…" "free," "act now!" and even greetings like "dear…" can trigger the filters.

While these are just a few examples, there are hundreds of words and expressions like this that can make email providers suspicious. Tools like OneShot can help you identify what kind of language has the potential to land your email in the spam folder.

Add Your Email Content to highlight Spam Words

Reading Time < 1 Min ✅   54 Words: Shorten Email ⚠️   Avoid Writing Long Sentences ⚠️   Ask a Question ⚠️

I : You Ratio is 4:0 ⚠️   SpamWords: 6 ⛔   Mobile Friendly ⛔

Dear friend ,

I am a Financial Consultant in control of privately owned funds placed for long term investments.

My client intends to invest these funds in projects. I am willing to finance projects at a guaranteed 5% ROI per annum for projects ranging from 2 years term and above but not exceeding 12 years.

Please answer ASAP.

🔴 urgent 🟠 shady 🟡 money 🟢 overpromise

🔵 unnatural 🔵 profanity

Best practice is to either remove spam trigger words entirely or use them sparingly and within context.
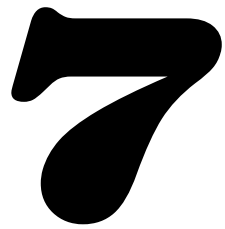
7 OPTIMIZE YOUR SUBJECT LINES

Your subject line won't directly affect deliverability.

(Unless you cram them with spam words, in which case you're likely headed to spam.)

But they do affect whether or not your email is opened.

Not only does an email need to be opened before it can be responded to (duh). But open rates are also a data point email servers look for to determine whether you're a reputable sender.

Needless to say, it's important to get them right.

There is TONS of advice on writing good subject lines. These are the most useful practices:

Keep your subject lines short: Countless data reports show subject lines between 1–3 words have the highest open rate. This is consistent with what we see with OneShot customers.

Make them look like an internal email: For two reasons. One, it doesn't look like a marketing email. Two, internal emails usually need to be acted upon, so if yours looks like one it'll increase the chances of it being opened.

Highlight one specific topic: Your subject line should reflect the theme of the email. Highlight the topic of yours in as few words as possible.

HERE ARE SOME EXAMPLES OF SOLID SUBJECT LINES:

✅ Low reply rates

✅ Ramping new reps

✅ Sequence templates

✅ Thoughts on personalization

AND HERE'S A FEW THINGS NOT TO INCLUDE:

❌ **Spam words & superlatives:** Free, better, improve, solution, accelerate, deal, best, etc.

❌ **Emojis:** Love 'em or hate 'em, in a subject line they reek of marketing. Best avoid.

❌ **First name:** Similar to the above, first names indicate you're being sold to.

❌ **Questions:** Save the ask for your call to action, not your subject line.

8 MONITOR FOR LOW OPEN RATES

Certain metrics are indicative of overall performance and worth keeping a close eye on. Open rate is one.

Your open rate is like a proxy for deliverability.

It's important to understand what good, and poor, open rates look like. For cold emails:

70%+ is excellent
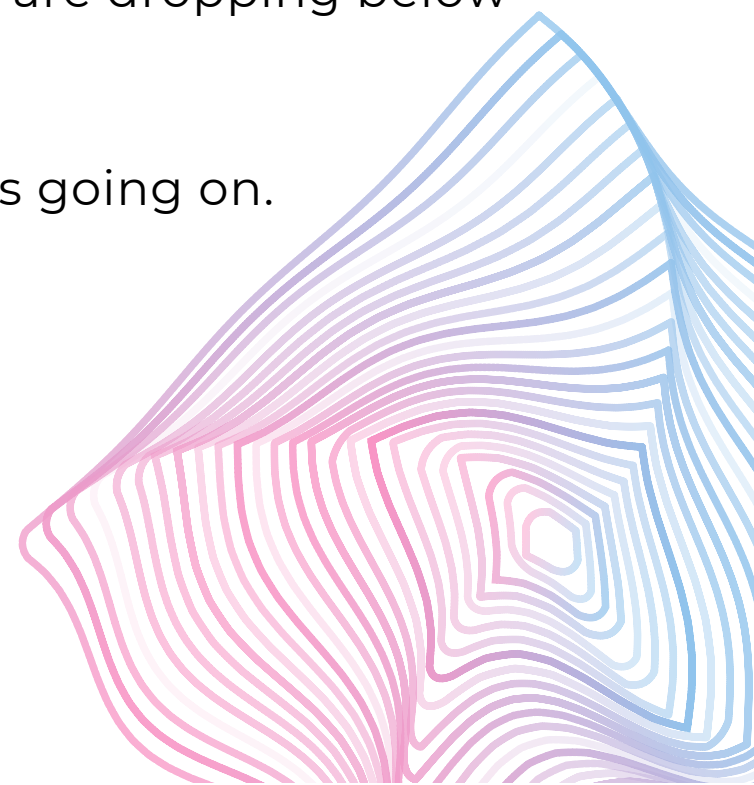
50-69% is solid and acceptable

<40% there could be an issue

The issue could be as benign and easily fixed as a bad subject line.

Or the low open could mean something more is serious going on, like problems with deliverability.
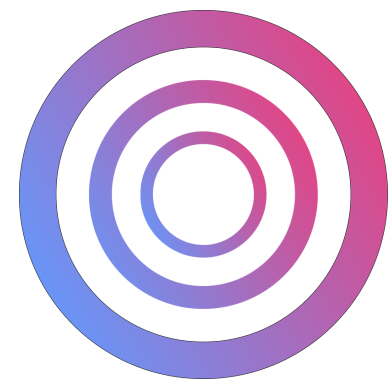
Closely monitor any emails and campaigns that are dropping below the ~40% threshold.

If they do slip, turn them off and look into what's going on.

9 PLAIN TEXT ONLY: REMOVE IMAGES, LINKS, AND TRACKING PIXELS

Excessive links, images, tracking pixels, and other complex elements in emails can negatively impact deliverability.

Because these elements can often trigger spam filters.

Also, emails full of images and custom code may not display properly across all devices and email clients.

Meaning your message may be illegible.

When cold prospecting, best practice is to send plain text emails.

They will format the same way across any device, and there are no links that may be deemed suspicious.

This simplicity enhances the **deliverability** and **readability** of your emails, improving their effectiveness.

But, there's a catch: no tracking.

Of course, the downside to this is the limited visibility into email performance.

With no tracking, you won't be able to observe the detailed performance of your campaigns.

No open rates. No click rates. No view counts.

However, there's a strong counter argument here: deliverability is more important than tracking.

The ultimate test of whether your campaigns are performing are the number of replies you receive. Which you'll always be able to see.

Bonus tip: Replace the unsubscribe link in your cold emails with a P.S. asking a recipient to ask to be taken off your list. This not only removes the link, but prompts a reply which can start a conversation.
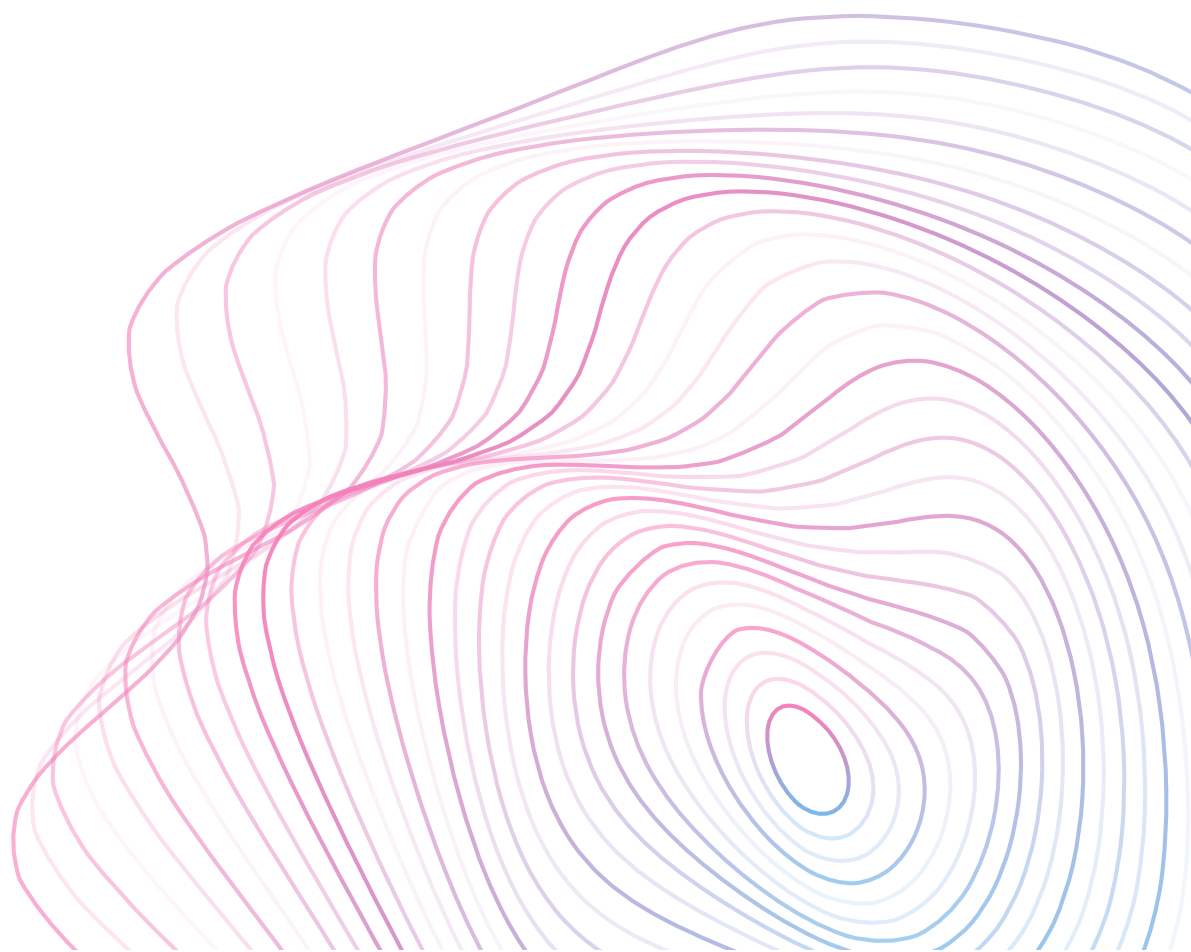
10 PERSONALIZE EACH EMAIL

Personalization is so important.

And not just to make your message more compelling to your prospect.

It's critical for deliverability, too.

When identical sales emails are sent to several recipients, email servers can flag this activity as spam or coming from a bot.

There are a couple of tactics to make each email you send slightly different to keep them off your back.

- **Spintax generators** (spintax = spin + syntax) slightly change the structure of what you've written so no two versions are exactly the same

- **Custom variables**, which are built into most email sending tools, allow you to add unique details like someone's name or company

- **Customize each message** so it's unique to the recipient.

The last one is the hardest. Especially when you're sending hundreds or even thousands of cold emails.

Personalization at scale used to be an oxymoron; and impossibility. At least until AI entered the chat.

Today, sophisticated AI can conduct deep research on a prospect and use the information it uncovers to automatically generate highly personalized outreach.

And it can do this hundreds of times, without getting tired.

Btw, that's what we've built at OneShot. If you want to see it in action you can check it out right here.

11 VALIDATE & VERIFY YOUR DATA

Each time an email is unable to be delivered, it's a hit to your domain.

Sometimes an email bounces because the email address isn't authentic, or no longer exists.

It's important to maintain clean prospect data to ensure your campaigns are only going to real, active email addresses.

Most sales teams will do a post-hoc cleanse.

Meaning after a campaign has run they'll look at the hard bounces and scrub the offending email addresses from the list.

Unfortunately, at this point the damage has already been done. Email providers have already dinged your domain.

There are lots of email verification tools on the market that check email addresses against factors like:

- **Syntax:** Are emails formatted correctly and free of typos
- **Domain verification:** Does the domain of the email address actually exist
- **Mail Exchanger (MX) Records:** Is this email address connected to the right server
- **SMTP Verification:** Does this specific email address exist on the server

Platforms like OneShot also automatically validate these factors before sending emails.

Whether you manually check your data or buy a tool to do it for you, data cleanliness is a critical factor in maintaining your email deliverability.

LOOK AT YOU, DELIVERABILITY PRO 😎

Those spam filters ain't got nothin' on you.

Armed with these tips, you'll be hitting the primary inbox (every time) in no time.

→ So, what's next?

Deliverability is a key piece of the prospecting puzzle.
But it's only one piece.

Good email prospecting can be a significant driver of revenue once you crack the code.

And if you keep at it long enough and keep experimenting and refining your approach, you WILL crack it.

At OneShot, our mission is to help you crack it faster.

Our AI-powered autonomous prospecting platform helps sales teams exponentially boost outbound productivity by automating all the repetitive tasks chewing into your reps' selling time:

→ Wave goodbye to the spam folder and land in the inbox every time with our intelligent delivery system

→ Use AI to find (and keep finding) great-fit leads from dozens of data sources in a fraction of the time

→ Research and reach out to prospects with superhuman speed and precision.

→ Create hyper-personalized outreach at scale that stands out and gets responses.

→ Automatically optimize and refine your approach with guidance from advanced machine learning.

In short, we help your sellers stop wasting time on prospecting tasks that can and should be automated and start getting back to actually selling.

Sound interesting?

Book a demo and see how we can put your prospecting on autopilot.

BOOK A DEMO

ONESHOT