Email Deliverability Risks & Best Practices: Avoid the Danger Zones
By: Amanda DeLuke

Why is email deliverability so important? It's how your emails get to your recipients' inboxes instead of ending up in the spam folder or being block-listed. Your hard work on your content and subject line will pay off when your email hits the inbox and is opened, but what if it doesn't make it that far?
You need to be informed about potential risks you're taking with your emails. Sometimes, you may not realize you were even taking a risk! Maintaining high deliverability during COVID-19 has been even more confusing, so it's more important than ever to stay up-to-date. Learn about the risks that can jeopardize your deliverability, and best practices you can follow to keep deliverability high.
I'll cover:

- Risky Email Deliverability Practices
- Email Deliverability Best Practices & Industry Trends
- Scoring Your Risks

Here's the bottom line:
Know the consequences when taking a risk and don't forget what their outcomes teach you.

12 RISKY EMAIL DELIVERABILITY PRACTICES

Let's dive into the **high-risk activities** that will jeopardize your email reaching the inbox.

1. Sending to Purchased/Rented/Leased/Shared Lists
Even if you're using list validation, buying, renting, or sharing an email list is a big no-no, and a risk you want to avoid. This practice is detrimental to your sender reputation and against our own rules of use.
Why? When you do this, you run the risk of taking down an entire sending system. You may feel comfortable with it using list validation, but list validation still isn't checking for consent of the individuals, doesn't find all the spam traps or honeypots, and may still be using role addresses (like name@xyz.org) which means you may not have proper consent for all individuals on that distribution list.
You know what they say… if something seems too good to be true, it probably is. While it may be tempting to send marketing emails to purchased lists of contacts, it's a major risk that you should avoid.

2. Volume Spikes
Sending out an email to a large group of addresses that you have never contacted before or haven't contacted in over three months is an example of a volume spike. You may have done this accidentally with a "happy holidays" email. Contacting unengaged email addresses like this out of the blue can cause your deliverability rate to plummet. I recommend maintaining consistency in your sending. If you're going to send to a list without recent engagement history, send the message more slowly and in smaller batches to gauge delivery rates before it causes harm to your sender reputation

3. Email Contains Mostly Images
Sending image-heavy or image-only emails is a huge red flag because it makes receivers think you're using a technique called image mapping. Spammers use image mapping to try to hide text within an image because it can't be scanned. If you want to use an image as the basis for your email, consider breaking up the image and putting some text beneath each image or putting the image into the header and putting text content into the body.

4. No Unsubscribe Mechanism
You want to have a clear, easy, compliant way for people to unsubscribe from your emails. I always tell people the worst thing that can happen to you is when someone marks you as spam – and if you don't have an obvious way to unsubscribe, watch out. You can bet that mail receivers, spam filters, and ISPs look at all that data.

5. Not Sending Mail from Your Organization's Domain
Avoid sending from domains like Gmail, Yahoo, etc. Why? These domains aren't owned or authenticated by you. It's best to use your own authenticated domain. There's a mechanism called DMARC that prevents people from using that domain outside of their system.

6. Exposed URLs
Using exposed URLS comes up a lot as a reason for email bounces. It's because if you include any type of tracking in your URLs and you hover over that URL, you're going to see the tracking URL, which is typically seen as a phishing attempt by spam appliances.
You want to make sure you cover your URL with text or an image. Here's an example of what this looks like:
Exposed URL *| Read our blog post: https://blog.higherlogic.com/improve-my-email-deliverability*
Recommended URL | *Find out how to improve your email deliverability*

7. Shortening Links
For dealing with long URLs, people often turn to third-party link shortening services (bit.ly and tinyurl.com), which convert long URLs to shorter versions that lead to the same landing page. Avoid these even if you're creating custom links.
Here's why you shouldn't use link shorteners in your email marketing content:

- They're typically block-listed by major block-list providers
- Spammers use these services to hide their destination URLs

Next, let's dive into our **medium-risk** categories.

8. Sending to Unengaged Individuals
When you send an email, you want to send to engaged subscribers. Why? You're more likely to have clicks, opens, replies, etc. on your email sends, indicating to the mail receivers that your emails are wanted. You want to send quality emails to people who are highly engaged – it's better for them, your deliverability rate, and engagement metrics. A good rule of thumb is to send to those who've actively engaged within the **past three months**.

If you receive pushback about this, keep in mind: You're only as strong as your weakest subscriber. If you send emails to recipients who aren't engaged, that person is just going to drag down your list and drag down your deliverability rate. Because they aren't opening your emails, you'll have low email engagement rates. ISPs and spam folders can see all that data, and they may notice that 20% of their list is not engaged. They conclude that people don't want it and send it to the spam filter.

9. Failure to Clean Lists Regularly

To help you avoid risk #8, establish a process to regularly clean your list. The first step is to ensure you have consent from the recipients on your email list. From there, I'd recommend taking a look at the last time those people engaged with you. If they haven't engaged with you for over three months, I would suppress them.

10. Sending Too Frequently

I define sending too frequently as sending to the same list more than once per day. Here's a common scenario of when you might see this. A sender makes a mistake on an email they've sent to their whole database – then they resend an email out with an "oops," causing a spike in volume. It's actually better for your deliverability in that situation to not send out the second email. I suggest waiting a day or even until the next morning to correct it. If you absolutely must send that second email, some automated email campaign platforms give you the ability to send on a distributed option so the emails go out in a staggered fashion, which can help.

11. Sending Attachments

Wondering if you should send attachments in your next marketing or communications email? The only safe attachment is a text file (.txt). So if you're attaching PDFs or any other file types, those can be marked as malicious and suspicious.

Consider these deliverability risks:

- Internet Service Providers (ISPs) may mark your attachment as spam
- Your subscriber may still think it's spam
- Your messages become too large
- Attachments get lost in the forwards

Rather than sending attachments, host the file online and link to it in your emails. By linking to the attachment you can reduce risk, improve the user experience, implement tracking, and increase the chances people will open and read your messages.

12. Spam-like content characteristics in the subject and body of the message

The list of spam-like characteristics is ever-changing, so periodically research the latest. You can expect it will include things like dollar signs, all caps, or certain types of punctuation. Spam filters will flag emails with these characteristics.

EMAIL DELIVERABILITY BEST PRACTICES

We've talked a lot about the bad stuff: Here's how to get those good results we want!
Best Practices to Follow for a Low-Risk Email

1. Get Authentication

Think of email authentication as a passport for traveling. As your emails travel through the internet, authentication proves to the receivers that you are who you say you are. SPF and DKIM are examples of types of email authentication.

Much like the average person doesn't answer a call from an unknown number, the average consumer inbox isn't going to trust an email from an unfamiliar or suspicious sender. Sender authentication is the foundation of email deliverability, as it helps identify an email's legitimacy while protecting against fraud, simplifying delivery, and building a positive domain reputation. Authenticating your "from" domain improves the credibility of your emails by implementing protocols that verify your domain as the sender of your messages.

2. Ask for Consent

You want to send *wanted* emails. To ensure your subscribers want to receive your emails, ask for their consent when they first sign up for your list, called double-opted in (DOI) or confirmed opted-in (COI). One idea for getting their consent is to send them a welcome email that asks them to take an action like clicking a link to verify their email.

3. Use Plain Text

With plain text emails, there isn't much to hide. Spam filters have an easier time accepting plain text emails because there are fewer places to hide nefarious elements. So make sure you take some time to review and adjust the text version of your HTML email because some strict filters will only accept the text version. Most .mil addresses only allow text emails to be received and some .gov and .edu addresses may have strict rules to only accept text versions of emails.

4. Have a Clear Unsubscribe Mechanism

This is the best practice version of one of our risks. Providing a clear unsubscribe mechanism and making sure it works is a great way to avoid becoming spam.

5. Proactively Unsubscribe

Ask your subscribers every so often if they're still interested and want to stay on your list. Think of this like when Netflix or YouTube asks, "Are you still there?" This helps you maintain an engaged list. I recommend asking about every three months. (Getting pushback? Remember, your email list is only as strong as your weakest subscriber.)

6. Send Highly Targeted and Relevant Content

Sending very specific content to a small list is a great way to maintain an engaged audience – and email deliverability. With good data (or integrated data) you can segment your audience and send those specific groups highly targeted messaging.

HOW AM I DOING? SCORING YOUR RISKS

You can find free email testing tools to see how risky your emails are. They'll check different elements of your email for spam risks and give you a score.

Another way to test your email deliverability is to create/use your own email account through Yahoo, AOL, Gmail, etc., and test sending your emails *to* those accounts (not *from* those accounts, remember, that's a risk factor). You can then check where they landed, which will help you understand where your recipients will get them.

Here's what you should test before sending your next email:

- Email design
- Accuracy of links
- Proof your content
- Images displaying properly
- Font and text displaying properly
- Virtual inbox/deliverability testing
- Functional unsubscribe mechanism

As a Deliverability Analyst at Higher Logic, Amanda DeLuke provides organizations with best sender practices, assists in improving deliverability/sender reputation, email authentication, manages mail servers, improving internal deliverability process, vetting and abuse desk, and email privacy and compliance.