Graduate Management Admission Council™

Email Best Practices: A Guide for GMAC™ GradSelect Users

Are Your Messages Reaching Your Audience?

Last Updated: May 2023

Deliverability Overview

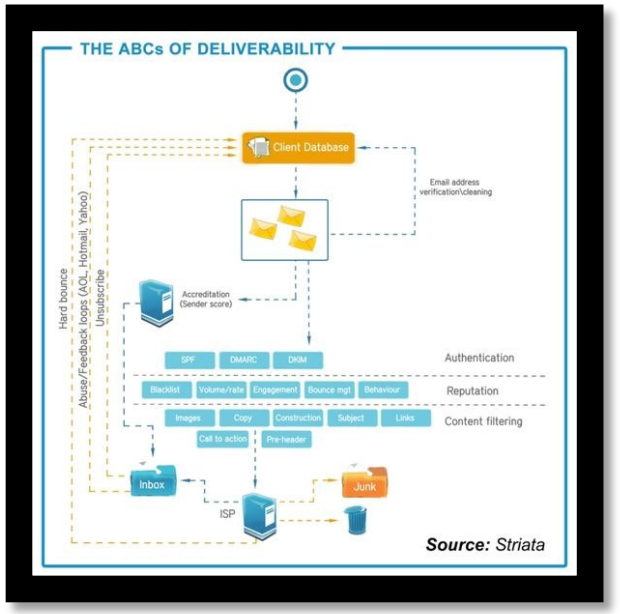
Did you know that up to 50% of emails sent to opted-in lists, never even make it to the inbox?

Internet Service Providers (ISPs) and email providers are using technologies to protect their users from receiving irrelevant, dangerous, or spam emails. It is necessary as an email marketer today, to understand how these systems work, and set up your systems to be recognized as a trusted and safe sender.

There are three main areas of deliverability to know: Reputation, Infrastructure, and Authentication.

These are explained in further detail on the appendix.

Reputation	Infrastructure	Authentication
Emails you send – and recipients' reactions – are tracked over time. If your reputation as a safe and welcome sender is damaged, emails may be blocked from reaching the inbox.	Dedicated IP addresses, secure servers, feedback loops, and the other best practices you need to use today.	DMARC, DKIM, and SPF are intimidating acronyms, but they are simply a way by which email providers validate that "you are who you say you are."



Source: bloomreach.com, blog.hubspot.com, returnpath.com, striata

Graduate Management Admission Council™

Deliverability = Reputation

Just as "brand equity" – or the value derived from your brand's reputation – is likely an important part of your school's marketing efforts, reputation is an important part of email deliverability. Here are some key metrics that ISPs look at to determine your sender reputation.

Proper Format
Ensure that emails are coded correctly to render properly – especially on multiple devices. Emails can be blocked if they would not show up correctly.

Consistent Volume
Sending a large batch of emails out of nowhere can be a red flag. Keep relatively consistent campaigns going year-round, and ISPs will be more likely to trust you. (Hint: a great way to do this is by setting up recurring searches in GradSelect)

Few Complaints
When recipients mark you as "junk" or "spam," those preferences don't go unnoticed. If too many people do this (more than 0.1%), your emails may not be delivered to others. Make sure your emails have a clear "unsubscribe" option for recipients to use to opt-out.

Avoiding "Spam Traps" and "Honeypots"
Spam traps and honeypots are deliberately set up by ISPs to "catch" senders who are practicing poor email hygiene, or getting leads from untrustworthy (and even illegal) sources. Fewer than 0.3% of GradSelect emails are flagged as potential problems.

Low Bounce Rates
Like spam rates, bounce rates are an indication that you are "out of touch" with your email recipients. The GradSelect database is cleaned to remove or update invalid email addresses – but be sure to do this for your other lead sources and remove or update bounced emails immediately.

No "Blacklist" Appearances
There are over 300 publicly available spam blacklists that range from the well known and more widely used lists created by credible companies to independent blacklists. Not all these blacklists are created equal; in fact, anyone can start a blacklist and decide what factors will result in being listed.

There are several places where you can check your email reputation, but Sender Score (**www.senderscore.org**) is among the most popular. Sender Score gives you a number on a scale from 0 to 100, with 90 and above considered a "good" reputation.

Deliverability = Infrastructure

In many organizations, there is a disconnect between marketers and IT specialists. There are a number of "checks" and systems that need to be set up to stay "up to code," and protect your email account(s) from hackers or other threats. Don't assume that this is all being done in the background for you – you are the email expert here!

Dedicated IP Address(es)
Your reputation is tied directly to your IP address, so avoid mixing purposes and dedicate an IP address just for your emails. Some marketers have separate IP addresses for advertising/promotions and transactional communications.

Secure Mail Servers
Just as with your company's website, cloud servers, data storage, etc., a mail server needs to meet certain requirements to be "secure" and protect from hackers/bots who could wreak havoc on your reputation and the privacy of your contacts.

ISP Feedback Loops
This is how you can address complaints from email recipients, and immediately remove anyone who unsubscribes. Continuing to email recipients who have requested you to stop will badly impact your deliverability. Note: Gmail's system is a bit different, requiring a "List-Unsubscribe" header instead.

"Postmaster" and "Abuse" Mailboxes
Many ISPs require that these be set up in order to access feedback loops (described above). If you don't have these set up and properly working, and actively monitored for complaints, you may be blocked.

Ability to Receive Mail
Fewer things are worse than receiving an email and seeing the sender as "DoNotReply".
Your sending domain needs to be able to receive mail, and monitored to ensure it is functioning properly.

Graduate Management Admission Council™

Deliverability = Authentication

Authentication is how ISPs determine that you are who you say you are, and not an impersonator running a phishing scam. It is similar to an "ID check" – but in the digital world, there are different protocols and systems for verifying your identity.

There are three important acronyms to understand:

- DKIM and SPF are technologies
- DMARC (Domain-based Message Authentication, Reporting & Conformance) is a protocol for using these technologies and used by all major ISPs

You likely will want to work with your IT department or email vendor to ensure that these methods are set up and working properly, but they are an essential part of email deliverability, and you should have an awareness and basic understanding of the setup and maintain it at regular intervals (e.g. monthly).

DKIM – Domain Keys Identified Mail
DKIM allows ISPs to verify that the content being sent is what the sender intended, and that the message doesn't get changed along the way.

Process:
• Sender publishes a "public key"
• Sender adds a "private key" on their mail servers and signs the message
• Receiving server/ISP checks private key against public key

Check your DKIM record here: https://dmarcian.com/dkim-inspector/

SPF – Sender Policy Framework
SPF tells ISPs which IP addresses are allowed to send messages on their behalf. It verifies that the message is coming from the right place and not an imposter. An "SPF record" is a line of text that might look like this: "v=spf1 ip4:12.34.56.78 include:example.com -all"

It is entered in a "txt record," and stored in the DNS (Domain Name System) and looked up and crosschecked by receiving mail servers.

Check your SPF record here: https://cauldron.dmarcian.com/spf-survey/

Graduate Management Admission Council™

Want More Information?

Click here to receive the entire Email Best Practices Guide

If you have any questions, click here to contact us directly at gmacconnect@gmac.com

Graduate Management Admission Council™

Source: campaignmonitor.com