SPF, DKIM, and DMARC

How to Setup and Why It's Crucial

by Thomas Petty, BOSS Academy Member

BOSS ACADEMY

THE LAST BOSS YOU'LL EVER NEED

How to Set Up SPF, DKIM, and DMARC and Why Its Crucial

by Thomas Petty

If I send a letter to my Aunt Mabel in Texas, I feel pretty confident that my letter will be delivered to her within a few days. The mail carrier doesn't really check who sent it, and if it has a stamp and a delivery address on it, it will be dropped in her mailbox.

Email is a different matter. As marketers, we want to make sure that our newsletters and regular emails get delivered to the intended recipient. But so often, our stuff gets sent to spam, and we don't feel like we have any control over that.

Worse, in February 2024, Google and Yahoo! both implemented tougher rules around email, and if you haven't implemented the new rules properly, it's MORE likely that your email newsletter will be banished to the spam heap.

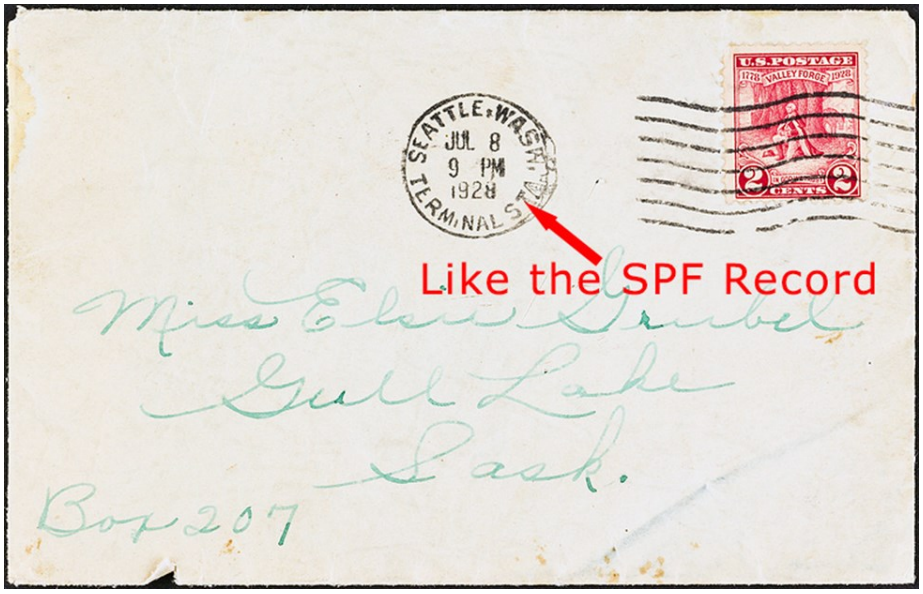
Who decides what is spam and what's not?

Well, it's complicated.

This article is intended to help you to understand the new rules as well as learn how the confusing alphabet soup of SPF, DKIM, and DMARC actually benefit you and your business. If they're set up correctly, your emails will more likely be delivered to your recipients.

What Is SPF?

Let's return to the letter I sent to Aunt Mabel. When I mail it, the local post office will cancel the stamp that says it's being mailed from my Zip Code, 95452.



Let's say that I tell the post office that I have a rule that I only want any mail that I send to come from 95452 or 95409, which is the next city over. If it gets sent (canceled) anywhere else, I didn't send it, and therefore, it's spam.

The SPF (Sender Policy Framework) is an email rule that's associated with your domain that defines where email can come from. It says something like, "Only email from Google and Constant Contact email servers are valid. Anything else is likely spam."

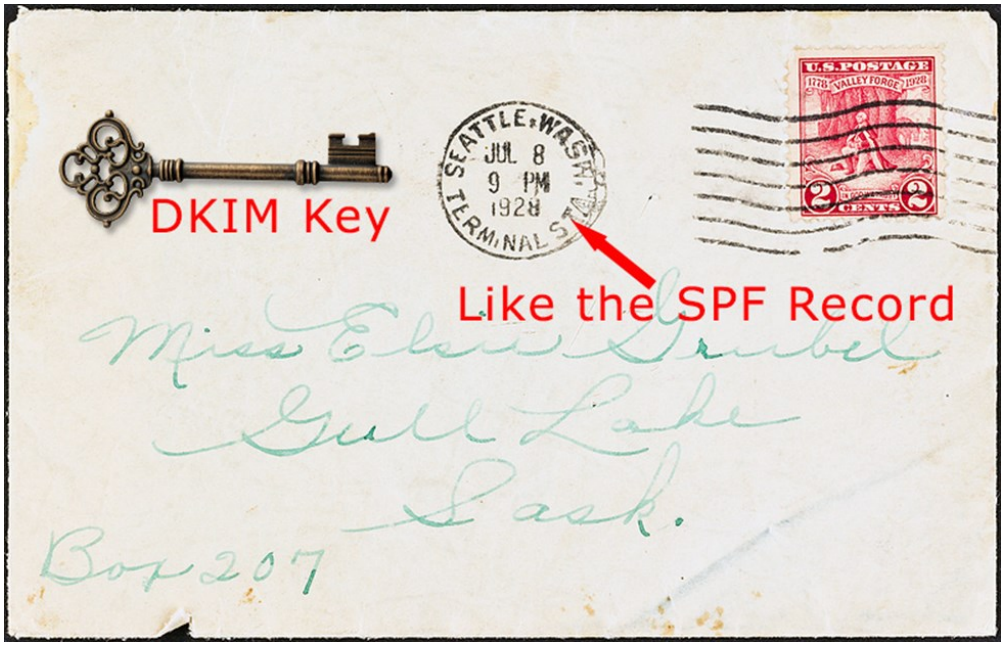
When the mail carrier tries to deliver my letter to Aunt Mabel, if the Zip Codes (i.e. the SPF record) don't match, she may put it in Aunt Mabel's spam folder instead.

So what if my next door neighbor decides to send a letter to Aunt Mabel, but addresses it from me? It will have the correct Zip Code cancelation mark, but there's no way to tell if it's spam or not.

This is the shortcoming of the SPF record. It's easy to spoof (fake) a sending email address, and the SPF record is public – anyone can read it – and spam emails will still get delivered.

What Is DKIM?

Now let's say that I tape a special kind of key onto the envelope. The poor mail carrier has to trudge all the way back to my house in California and test the key to see if it fits in a lock that's unique to my house.



If the key fits, then it's even more likely that the email really came from me, because my neighbor doesn't have that special key.

DKIM (Domain Keys Identified Mail) is a combination of a public key (like the one I taped to the envelope), and a private key (the lock on my house). No one else has the private key, and it's impossible to duplicate.

This is like young John Connor and Miles Dyson in the movie Terminator 2 when they both had to turn a separate key at the same time before they could get the Terminator's brain chip and robot arm out of a vault.

If my email's DKIM key matches the private key, this almost guarantees that the mail I'm sending really is coming from me or one of my systems.

When combined with a positive SPF record, the mail carrier will feel confident that the letter is legit and deliver it.

What is DMARC?

Returning to my letter to Aunt Mabel, when the poor mail carrier comes all the way back to my house to test the DKIM key, I'll have a note taped to the house with rules about what I want the mail carrier to do with letter, depending on whether DKIM and/or SPF passed.

She can deliver it no matter what (i.e. do nothing different), put it in the spam folder if one or both rules don't pass (quarantine), or put it in the trash (reject).

DMARC (Domain-Based Message Authentication, Reporting & Conformance) is like the rule that I've got taped to my house. The receiving email server will check SPF and DKIM, then look to see what rules I've set up before deciding what to do with the email I've sent.

What Systems Send Email "From" Your Domain?

You need to create a complete inventory of all the places that email comes from your domain, like fred@example.com, sales@example.com, or info@example.com. If it has your domain attached to the email address (not @gmail.com or @hotmail.com), then you need to list it.

Examples include:

- GSuite for Business (Google) or Outlook 365 (Microsoft)
- Your POP/IMAP server – Bluehost, GoDaddy, Host Gator, Network Solutions, iCloud, etc.
- Your web server – contact us forms, subscribe forms, lead magnet forms, etc.
- Your email newsletter – Constant Contact, Mailchimp, GetResponse, Klaviyo, etc.
- Your sales funnels – LeadPages, Click Funnels, Kajabi, etc.
- Learning Management Systems (LMS) – Teachable, Thinkific, Ruzuku, etc.
- Customer Relationship Managers (CRM) – Ontraport, Salesforce, Kajabi, Hubspot, etc.

Write them all down so you have a record of everything.

Google how to set up SPF and DKIM for each platform and make note of the step-by-step instructions. Some systems like Constant Contact are fairly easy to set up. Others like Google's GSuite are a bit more complicated.

Add these URLs to your list.

Edit or Set Up Your DNS Records

Next, you'll need access to where your DNS (Domain Name Server) records are kept. In many cases, it'll be on your domain registrar's site, like GoDaddy or Network Solutions. However, if you've switched to Cloudflare, AWS or some other system, you'll need to get access there.

Please note: **If you are not comfortable or familiar with making DNS changes do not try to "figure it out".** You can seriously booger things up (that's a technical term).

Work with your IT support people or **contact Thomas Petty** **directly** to get it done correctly.

ALWAYS back up or make a copy of your DNS records, which is called your Zone File. Most DNS providers give you an option to export your Zone File. DO THIS BEFORE YOU DO ANYTHING ELSE and save it to your computer so you can get things back up in case you or your IT company "boogers it up".

Follow the instructions to set up the SPF and DKIM records or work with your expert to set them up.

Note that you can only have one SPF record, and a mistake I've sometimes seen is that a domain has more than one SPF record. This needs an experienced person to consolidate the records correctly.

Set Up DMARC

A lot of the platforms will tell you to set up a default DMARC record that looks like this:

v=DMARC1; p=none;

The "p=none;" parameter is telling the receiving email server that "no matter if SPF and DKIM match or fail, go ahead and deliver it anyway" or "do nothing".

This in my opinion, is incorrect, because it's not going to report anything back to you or anyone else. It's like sticking your head in the sand. I also suspect that Google will flag this DMARC record in the future as inadequate.

You need to monitor successes or failures to know where emails are coming from and whether they're being delivered or not. If you don't want to do that, work with someone who knows how to interpret the reports and get it working correctly over time.

It's OK to start with the "p=none;" parameter for now, but you need to modify the DMARC rule to set up a reporting tool to decipher all the hundreds of reports you're going to get back.

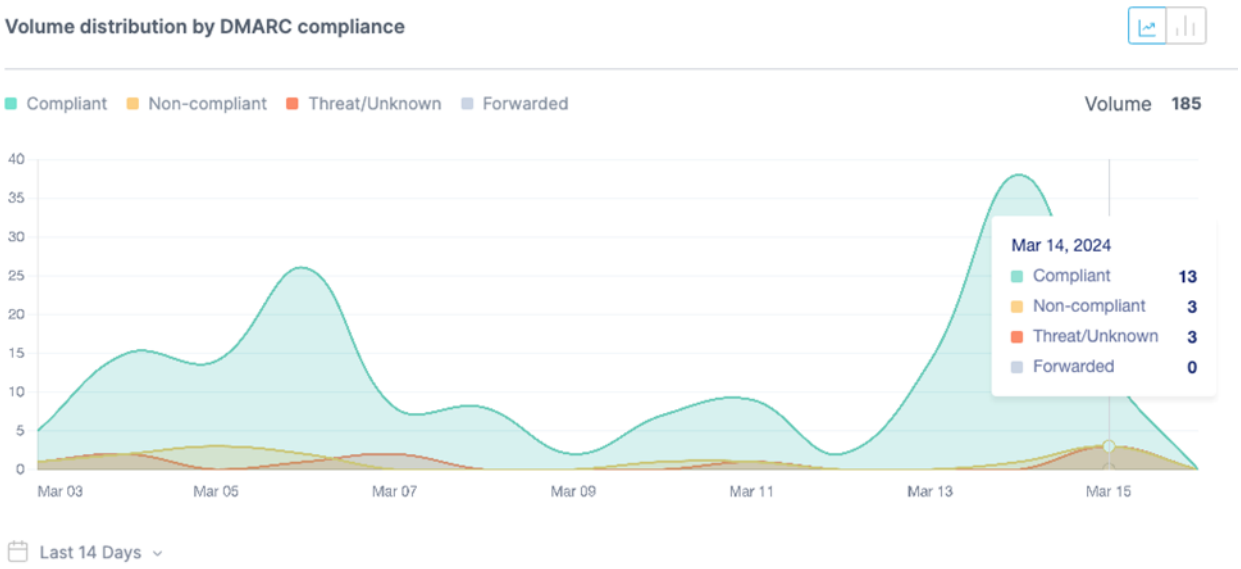
Then you can graduate over time to "p=quarantine;" and ultimately, "p=reject;" after you know everything is working perfectly.

Cloudflare's DMARC reporting is available free of charge if you use them. They will tell you how to modify or set up the DMARC record, and with the click of a button, they'll do it for you.

If you're using a different DNS platform, EasyDMARC will help you get it set up correctly.

I've been using EasyDMARC for a while now, and it works well to help me decipher all the reports. They have a free version and a paid version which provides even more data and reporting options. If you're a small business or solopreneur, the free version is just fine.

They will tell you exactly how to set up the DMARC record so they receive all your data and start producing the graphs and charts that will help you determine what's working or not.



I discovered that spammers in Russia are using my email address to send spam (those are the "Threat/Unknown" emails).

Ugh…

Now I can lock it down so their garbage automatically gets nuked.

Conclusion

Most of us feel like we really don't have a lot of control over whether our marketing (and real) emails get delivered to the recipient's Inbox or to the spam folder.

But if you set up your SPF, DKIM, and DMARC records correctly, this will ensure that legitimate emails get to where they're supposed to, and the spammers go straight into a black hole.

About Thomas Petty

Thomas has been a WordPress web developer and security consultant for over ten years. He's worked with solopreneurs, non-profits, Fortune 500 companies, and large government contractors to secure their websites and set up their DNS correctly.

Before that, he worked in IT and server support for a Fortune 100 company for over twenty years.

He can be reached at 925-245-0216 or via email through his website