Session-8: DKIM, SPF, introduction to email forensics.

This is serious. This is about your email deliverability. I know from my own experience that these acronyms may sound unfamiliar, scary and may seem totally uninteresting. Or maybe they sound familiar, but you never cared enough to check what they really are.

Either way, it's time to learn a bit about SPF & DKIM and set them up in your DNS records for your mail server, if you want to have a better control over your email deliverability.

What is SPF?

Simply speaking, Sender Policy Framework (SPF) is a security mechanism created to prevent the bad guys from sending emails in your behalf. The mechanism is all about communication between DNS servers… and this is the point when it all starts to sound scary! But don't panic. I'll try to keep it as simple as possible.

Let's say you've sent an email to Bob. But how does Bob's DNS server know that the email was in fact sent by you? The problem is, it doesn't really. Unless you have SPF set on your DNS server.

SPF defines which IP addresses can be used to send emails from your domain. So let's imagine two possible server "conversations". To make it all easier, let's assume your name is Mike.

Scenario 1 – You don't have SPF set up.

Mike's server: Hey, Bob's server. I've got a new message from Mike.
Bob's server: Hi Mike's server. What's your SPF?
Mike's server: Yeah, about the SPF… Who cares, really. I don't have one. Trust me, it's from Mike.
Bob's server: If you don't have SPF, I can't be sure it was Mike who sent this. Give me Mike's allowed IPs, so I can compare it with yours.
Mike's server: I don't have the list of Mike's allowed IPs.
Bob's server: Then I don't want your message. Delivery denied. Sorry, buddy…

Scenario 2 – You do have SPF set up.

Mike's server: Hey, Bob's server. I've got a new message from Mike.
Bob's server: Hi Mike's server. What's your SPF?
Mike's server: There you go, here's my SPF. There's a whole list of IPs that Mike himself declared as the ones which can be used on his behalf.
Bob's server: Ok, let me see… And the message you have for me is sent from IP 64.233.160.19. Ok, it's on the list. Everything looks fine. Gimme the message, I'll show it to Bob. Thanks!

My apologies to all tech-savvy readers of this blog for this ignorant oversimplification. Please forgive us dummies, and keep in mind that we do envy you your super-analytical minds.

Anyway, the moral of those two short dialogues is: set your SPF. If you don't, you may look like a bad guy, and not all your emails will be delivered.

How to set SPF on your server?

The general idea is to make sure all applications that send emails on your behalf (and are using their own SMTP, not yours) are included in your SPF. For instance, if you're using Google Apps to send emails from your domain, you should put Google in your SPF. Here's Google's instruction on how to do this.

But it's important to make sure, if Google is the only app that you should "allow" in your SPF. For instance, we're using HelpScout to manage our support emails and MailChimp to send our newsletters. We include both of them in our SPF.

Oh, so should I include Woodpecker in my SPF as well?

No. Like I mentioned, you should remember to put into your SPF record the apps that send emails on your behalf, but are using their own SMTP. Woodpecker uses your SMTP to send your emails, so it's more of an online email client with super powers than a mass email sending app.

That said, the deliverability of the emails sent from Woodpecker depends on the reputation of your domain. Setting SPF and DKIM will help you protect the good reputation of your domain, and thus improve the deliverability of your emails.

First step to setting up your SPF

The first step is to check what is your current SPF. You can do that using tools like:

- MxToolbox
- Google Apps Toolbox

When you type in your domain there (for instance I would type in woodpecker.co), the tools will run some tests and show you your current SPF, or a notification that it hasn't been set yet.

What are the next steps?

It's almost impossible to prepare a step by step tutorial for this, because this is something you set up in the administrative console for your domain. Depending on your domain host, the steps will differ. Basically, it's about pasting a properly structured line of text in the right place in the console.

For instance, if you are using Google Apps to send all emails from your domain, the line would look like this:

"v=spf1 include:_spf.google.com ~all"

The "**v=spf1**" part of the record is called the version, and the ones that come after that are called mechanisms.

Now let's see what each parts means exactly.

1. **v=spf1** this element identifies the record as an SPF
2. **include:_spf.google.com** this mechanism includes mail servers that are authorized servers
3. **~all** this one indicates that if an email is received from an unauthorized (not listed in the "include:" mechanism) server, it gets tagged as soft fail, which means it can be let through, but could be flagged as spam or suspicious.

But if you're using more apps than that (for instance something to send your newsletter, something to send your support messages, etc.), the line will be a bit longer, because you will have to include all the other apps in it. Or if you don't use Google Apps but a server from another host, for instance GoDaddy, the line will look different.

Here's how to set SPF in the most common domain hosts:

- Google
- Microsoft
- Zoho
- NameCheap
- GoDaddy
- Amazon SES

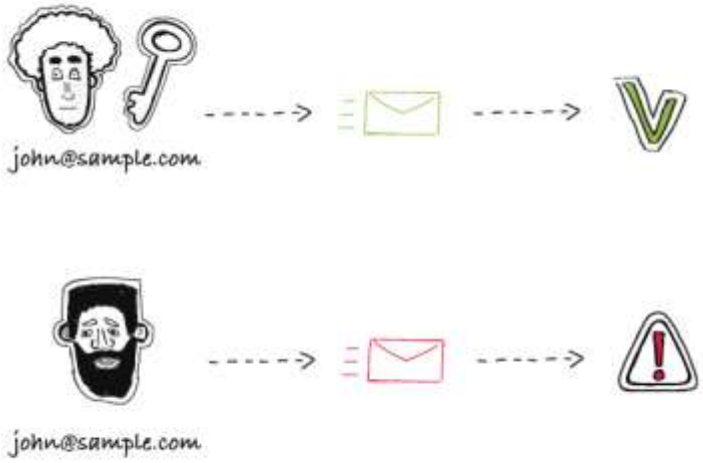
The best idea is to ask someone tech-savvy for help here. They will know how to formulate the text and they will quickly find the right place to paste it.

If you're currently using or testing Woodpecker and you're not sure if your SPF is properly set, you may check it directly in the app: go to SETTINGS > EMAIL ACCOUNTS > DELIVERABILITY (on the left-hand side) or contact us at support@woodpecker.co to get some individual help.

What is DKIM?

DomainKeys Identified Mail (DKIM) standard has been created for the same reason as SPF: to prevent the bad guys from impersonating you as an email sender. It's a way to additionally sign your emails in a way that will allow the recipient's server check if the sender was really you or not.

By setting DKIM on your DNS server, you're adding additional way to tell your receivers "yes, it's really me who's sending this message".



The whole idea is based on encrypting and decrypting the additional signature, put in the header of your message. To make that possible, you need to have two keys:

- the **private key** (which is unique to your domain and available exclusively to you. It allows you to encrypt your signature in the header of your messages.)

- the **public key** (which you add to your DNS records using DKIM standard, in order to allow your recipient's server retrieve it and decrypt your hidden signature from the header of your message).

Take Game of Thrones to get the bigger picture of DKIM. Ned Stark is sending a raven with a message to king Robert. Everyone could take a piece of paper, write a message and sign it Ned Stark. But there's a way to authenticate the message – the seal. Now, everyone knows that Ned's seal is a direwolf (that's the public key). But only Ned has the original seal and can set it on his messages (that's the private key).

Setting DKIM is just putting the information about the public key into your server's records. It is also a txt record that needs to be put in the right place.

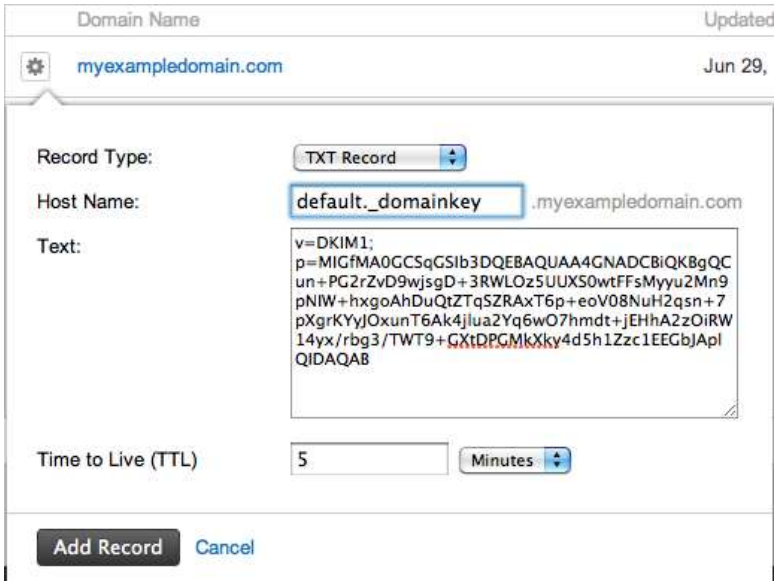
Once you have set that up, each time someone gets an email from you, the receiver's server will try to decrypt your hidden signature using the public key. If it succeeds, this will additionally authenticate your message and in result increase the deliverability of all your emails.

How to set DKIM on your server?

First, you need to generate the public key. To do that, you need to log in to your email's provider admin console. The next steps may differ depending on your email provider.

If you're using Google Apps to send your emails, here's a step-by-step instruction. Google Apps email users, you should know that on default the DKIM signatures are turned off, so you need to turn them on manually in your Google Admin console.

When you have the public key, you take the generated txt record and paste it in the right place into your DNS records.



Finally, you need to turn on email signing to start sending emails including your signature encrypted with your private key. Here's how to do it, if you're using Google Apps to send your emails.

Here's how to set DKIM in some of the other domain hosts:

- Microsoft
- Zoho
- NameCheap

Again, the best idea is to ask someone tech-savvy for some help with this. They will know or quickly find out how to generate the key and where to set everything up to make DKIM work properly for you.

If you're currently using Woodpecker and don't have an IT person to ask for help with SPF and DKIM settings, you may contact us at support@woodpecker.co for some individual help.

If you'd like to check if your SPF and DKIM are set up properly, you may do so in the app: go to SETTINGS > EMAIL ACCOUNTS > DELIVERABILITY (on the left-hand side).

Final words

If you're sending lots of emails, whether it's for marketing or for inbound or outbound sales, the reputation of your domain is crucial and you should take really good care of it. You don't want your domain to get on a blacklist and your emails to end up in spam. Setting SPF and DKIM records properly on your DNS server is a necessary step towards the security of your domain and high deliverability of your messages.

Setting it up may seem complicated, but it's undoubtedly worth the effort. If I were you, I'd go to my Woodpecker account and check if my SPF and DKIM are properly set right now or ask my IT guys to do it (if you're not a Woodpecker user). And if it turned out that the answer is "no", I'd ask them to help me out. And I wouldn't let them to fob me off. Not with this one.