RELIABLE AND TRUSTED EMAIL COMMUNICATIONS - SHEDDING SOME LIGHT ON CONFIGURING AND MANAGING SPF, DKIM, AND DMARC.

By: BRIAN PLATZ

Email services used to be one of the most reliable internet services. An Email sent resulted in either (**1**) a positive delivery of that Email or (**2**) the return of an error message – Simple; Right?

Email, and how it is delivered today, has **DRASTICALLY changed** due to the many malicious players out there. This has forced domain owners to take extra actions to protect their domain and assure their email is **"Reliable and Trusted"**. This article tries to shed some light on the overall topic. The topic is very complicated; even for techie folks, but it is a very important one right now.

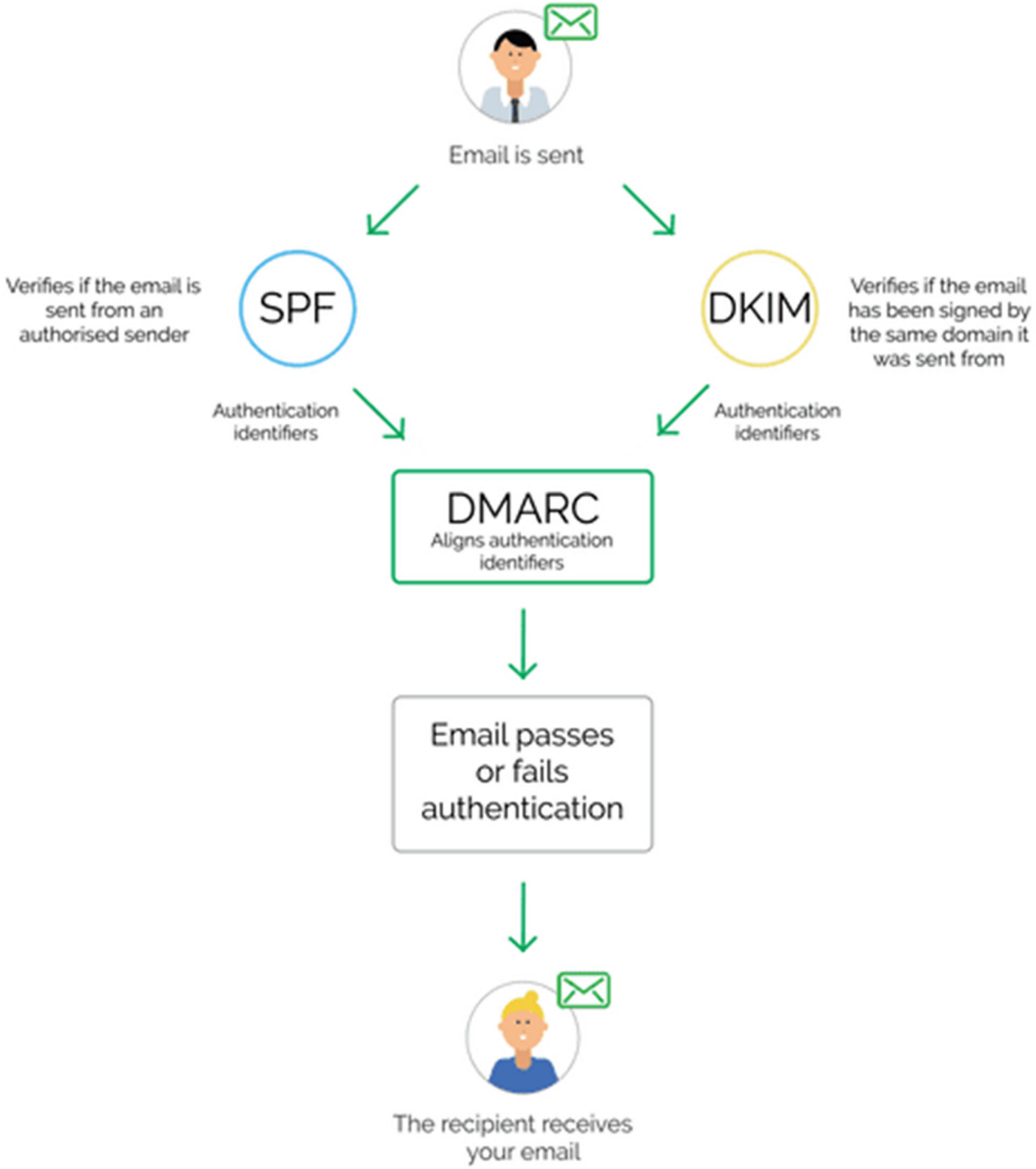
Email is a critical part of your business. You use it to communicate with customers, suppliers and partners on a daily basis for your company to function and to stay profitable. At one time all you required was a mail server a few MX Records and you could send and receive emails all day long.

Now, because of phishing attacks you require spam filters and SSL certificates along with other technologies to deal effectively with your business emails. Domain spoofing is a common form of phishing. It occurs when an attacker appears to use a company's domain to impersonate a company or one of its employees such as sending invoices that appear to come from your domain. There are three key advance technologies being used now to combat phishing:

- **SPF (Sender Policy Framework)**
- **DKIM (Domain Keys Identified Mail)**
- **DMARC (Domain-Based Message Authentication)**

HERE`S HOW AN SPF RECORD WORKS WHEN AN EMAIL IS SENT TO A CUSTOMER:

1. The email server with an IP address of 52.96.200.50 sends a message from info@**mycompanydomain.com** to customer@**xyz.com**.
2. The email server for **xyz.com** checks the SPF record for **mycompanydomain.com** to see if 52.96.200.50 "is allowed" to send emails on behalf of **mycompanydomain.com**.
3. If the SPF record lists 52.96.200.50 for **mycompanydomain.com** it "allows delivery" from the IP address 52.96.200.50 and the customer receives the message.



SPF – (SENDER POLICY FRAMEWORK)

Phishing involves sending fake emails by impersonating a sender. SPF helps weed out abusive emails and detect forgery. It allows recipients to verify sender identity (at the organizational level) by allowing domain owners to publish, via DNS, what mail servers “are authorized” to send emails from the specified domains. SPF also allows domain owners to specify email sending policies—such as what recipient email servers should do with an email that fails an SPF check. SPF requires domain owners to make this information available in an SPF DNS record. When the recipient’s email server gets the message, it “checks the authenticity” of the sender’s address to see if it matches the published list of email servers (IP addresses) in the domain owner’s SPF records. If this does not check out properly, the email message can be construed as forged. This is a very important layer of protection.

How should my SPF record look?

Your SPF record might look different depending on how you want it to behave. If you send mail using multiple email services (like third-party email marketing products), your SPF record needs to include those services as well. Contact your provider to find out what their SPF record should be.

DKIM – (DOMAINKEYS IDENTIFIED MAIL)

DKIM takes email sender identification a step further by associating a domain name and owner to the content of the email message, allowing the organization to vouch for the content of the message. This is accomplished by cryptographic signing of the content. Therefore, if you want to send a DKIM-signed message, your email administrator can implement a DKIM signing agent. Once available, the signing agent generates a cryptographic key pair— one private, one public. The private key is used by the signing agent to sign messages coming from your organization. The public key is made available to recipients via special DKIM-specific DNS records. The receiving organization can then use the public key to verify the signature, thus giving them a firm determinant as to whether or not the message content is vouched for by the sending domain's owner. The signature verification also facilitates the receiving organization's ability to make sure that no one altered the signed portions of the message while it was on its path to the recipient. It can be a reliable method of verifying a sender. As DKIM.org suggests, "Receivers who successfully validate a signature can use information about the signer as part of a program to limit spam, spoofing, phishing, or other undesirable behavior.

The reason DKIM alone is not a good basis for spam detection is that it's easy for spammers to set up and use DKIM just like anyone else. A better, more robust choice is deployment of an email security solution with options that allow you to deliver, tag, or deny a subject in certain situations: "when a DKIM signature is present but not valid," when "no DKIM signature is present," or when "a valid DKIM signature is present." And even better is a solution that includes message reputation services that identify email messages carrying malicious payloads—even if the sources appear to be reputable, such as whitelisted companies.

DMARC – (DOMAIN-BASED MESSAGE AUTHENTICATION)

DMARC improves on SPF and DKIM by giving sending organizations a stronger means of communicating the confidence of their SPF and DKIM implementations and by providing a framework for receiving organizations to provide feedback to sending organizations, including detailed information on who is attempting to spoof sender domains.

DMARC leverages SPF and DKIM, but unlike these two authentication methods, DMARC enables domain owners to publish policies that can be considered by recipients when handling SPF and DKIM failures. Policy actions can include: do nothing at all, quarantine, or reject the spoofed email. These types of policies significantly reduce user exposure to fraudulent and potentially malicious email. Most importantly, with DMARC, email receivers can report back to sender's critical data about the messages that pass or fail DMARC authentication, so that senders can take the appropriate steps to improve their sending posture. For example, using DMARC feedback, an organization may determine that there are valid IP ranges that are not included in their SPF records, allowing them to update the records and increase the accuracy of their DMARC posture.

DMARC DOES A FEW THINGS:

1. It considers the results from SPF and DKIM
2. It requires not only for SPF or DKIM to pass but for the domain used by either one to also align with the domain found in the **From address** in order for DMARC to pass.
3. It reports SPF, DKIM and DMARC results back to the domain found in the **From address** (ie. sender).
4. It tells receivers how to treat emails that fail DMARC validation by specifying a policy in DNS.

CONCLUSION

Just because you have implemented some or all of these email sender identity technologies doesn't mean you are covered. It's important to thoroughly understand the limitations and best practices to solve the problem you are grappling with. Ultimately, every company is a sender and a receiver. It's in everyone's best interest to keep raising the bar on email security by properly and diligently implementing email sender identity technologies to cover all the bases and prevent phishing or spear-phishing campaigns from opening the door to malicious threats that could compromise sensitive data and business operations. Business owners should be making efforts to improve their company emails sent are reputable, reliable and trusted and are protected against known and emerging malware-based threats.

ADDITIONAL LINKS

- More on SPF Record Syntax → http://www.open-spf.org/SPF_Record_Syntax/
- More about DKIM Records → http://dkim.org/
- More about DMARC Records → https://dmarc.org/

Brian Platz is the Web Doctor; an internet consultant living in Salem, Oregon since 1996.
We can help you analyze, implement and properly align your domain's **SPF, DKIM and DMARC** making sure your companies email delivery is **reliable and trusted**.

View a number of other informative, technical articles on our web site.
https://www.DBWebDoctor.com/Articles.asp