SPF, DKIM, and DMARC Demystified
The what, why, and how of email sender identity technologies

Enterprise sender identity technologies—SPF, DKIM, and DMARC—when properly implemented and incorporated into your email security strategy, can go a long way toward securing email, your most valuable business communication tool. Phishing and spear-phishing not only trick your employees, your partners, and your customers into revealing their personal and financial information, they can also lead to the introduction of stealthy malware that could compromise corporate intellectual property and other vital data assets. But there is a ray of hope.

Spear-Phishing Cracks Open the Corporate Gates
Beyond duping individuals and undermining the reliability of email as a communication tool (even internal email communications), phishing in all of its permutations is another method fraudsters have added to the mix of multi-vector, advanced persistent threats (APTs) that plague businesses and government agencies today.

As Information Security Magazine suggests, hackers have graduated from simple phishing techniques to spear-phishing techniques. Sophisticated cybercriminals use social engineering to gather specific information on their targets: individuals and groups are profiled based on information mined from social media networks or cloud-based shared document applications. “Spear-phishing focuses on an individual or small group of individuals and delivers a personalized lure—often using intelligence gleaned from social networks—designed specifically for those individuals.”

At times, spear-phishing messages contain malicious attachments in the form of ZIP files that appear to be Microsoft Excel files, RTFs, or PDFs to disguise the .EXE file extension, which is generally blocked by email security programs. An example is spear-phishing emails that masquerade as official notices from well-known delivery services, internal technical support, the Better Business Bureau, and even the Federal Trade Commission (FTC).
Other variations entice unsuspecting employees to click on URLs where bad code is downloaded. For example, in January 2013, The New York Times was victimized by a spear-phishing campaign that stole passwords and compromised the PCs of 53 employees, including the bureau chief. Fortunately, the attack was intercepted, and apparently no valuable documents were appropriated. Of course, it could have been much, much worse.2

And then there are sites that harvest valuable personal or financial data. The goal is to lead victims to legitimate-looking websites that ask for logins, passwords, credit card numbers, and other information. These sites often look quite convincing, with the same imagery and branding of real organizations. Often, the spear-phishing emails containing the malicious links look as if they came from an internal source, like the CEO of a company you work for, or other trusted sender.
Aside from training employees in email security awareness and strong firewall protection, there are technologies available today that help you protect your organization specifically against spear-phishing. There are three public domain frameworks available to everyone: SPF, DKIM, and DMARC. Let’s take a look at how each one works and how they assist organizations with authentication of email senders.

**Email Sender Identity Technology Basics**

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, the IP addresses that are authorized to send emails from the specified domains. SPF also allows domain owners to specify email sending policies—such as what recipients should do with an email that fails an SPF check. SPF requires domain owners to make this information available in an SPF .TXT record in their domain name server (DNS). 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 IP address in the domain owner’s SPF records. If this does not check out properly, the email message can be construed as forged. Not all email servers support SPF. However, this important layer of protection is provided by the McAfee® Email Protection solutions.

**Sender policy framework (SPF)**

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, such as the McAfee Email Protection solutions. 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 .TXT records.
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 is important to note that DKIM by itself isn't a good way to determine whether messages are spam, but 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, although the DKIM specification itself does not prescribe any specific actions by the recipient.”

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 appears to be reputable, such as whitelisted companies.

Domain-Based Message Authentication (DMARC)
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 senders 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.

Technology Limitations and Risks
While SPF, DKIM, and DMARC offer hope to many enterprises, there are some limitations:

- Although estimates vary, these technologies have not been widely implemented by organizations. Of those that have, many have inaccurate implementations. DMARC is a step forward in helping organizations implement SPF in an accurate manner, thanks to its feedback mechanisms, but translating the feedback into actionable data can be time consuming and costly.
- Because so many organizations' SPF records are inaccurate, most are hesitant to block an email just because it fails an SPF check. Therefore, a great deal of the potential value is lost.
- In multi-tenant email environments, IP space across customers is usually shared—and, therefore, SPF records are also shared. This makes it virtually impossible for SPF to be used to effectively tell the difference between one sender and the next on the same hosted platform.
• DKIM also has its shortcomings. For example, forwarded messages from list servers, which might be perfectly harmless—such as alumni.hbs.edu—could fail a DKIM check because the list server modifies the message before relaying it on. The simple act of adding an outbound disclaimer after the DKIM signature is in place can render the signature invalid. So the rule of thumb is: DKIM signing should occur after no further data operations will be applied to the message.

• SPF, DKIM, and DMARC are virtually ineffective in preventing phishing attempts that use domain names owned by cybercriminals that may appear legitimate to a user. For example, a domain like chasebankonline.com may appear completely safe and authentic to a user, but it might, in fact, be owned by a spammer who has fully implemented DMARC, SPF, and DKIM.

• DMARC can only be as effective as its foundational SPF and DKIM underpinnings. Without proper SPF and DKIM records, DMARC can impede your ability to successfully deliver mail. For example, let’s say the marketing department at your organization contracts with a third party to send invitations to webinars to a customer mailing list and these invitations appear to come from webinar@yourcompany.com. Because your IT department has no knowledge that a third-party is sending emails out on behalf of your company from the third party’s servers and using its sender identification, the emails may never get delivered.

There are certain risks in adopting any or all of the standards we have discussed:

• As a receiving organization, taking an aggressive policy on failed SPF/DKIM may result in an increase in false positives, causing you to drop otherwise perfectly good email. You need to consider how that might affect business operations.

• As a receiving organization, enforcing a sender’s DMARC policy means you trust their strategy. You need to consider, for example, whether a financial institution would take a more aggressive stance compared to a retail organization. The latter’s business model, for example, may be more heavily dependent on deliverability, with the goal of driving traffic to its website, so the retailer might have a more relaxed policy and would prefer to have fewer false positives.

• You are also trusting vendors to actively monitor the spoofing attacks on their sites and update their DMARC records accordingly. If senders are lax about their policies, that may mean your company is exposed and vulnerable to hackers who are adept at exploiting the gaps. With that in mind, it would be a good idea to find out what percentage of email senders use SPF, DKIM, and DMARC.

Adoption rate of these technologies has room to improve despite how long SPF and DKIM have been around, which leaves many messages unauthenticated and mail servers unlisted. DMARC supporters argue that low adoption is due to lack of sufficient data being available to implementers—a problem DMARC solves. DMARC makes the following information readily available to domain owners, including:

• Relative levels of spoofing of your domain(s).

• Who (sender IPs) is spoofing you.

• What non-internal senders are legally spoofing your domain(s).
Best Practices
In spite of some of the shortcomings of email sender identity technologies, it would be prudent to implement these standards properly to reduce your risk. You first need to get your SPF and DKIM records in order. It's critical to do things in the right order. Without this important step, DMARC can wreak havoc on your ability to successfully deliver email. If you are a major retailer, financial institution, a business that is frequently spoofed by phishers, or a business that cannot implement SPF because you don't have a firm grasp on all the senders allowed to send as your domain(s), implement DMARC and begin the process of obtaining DMARC report data. Adjust your records and send policies accordingly.

In the case of verifying inbound email, consider targeting your SPF and DKIM enforcement to those domains of your major business partners that you know have properly implemented these technologies.

But what if you have already implemented all three technologies? It doesn't end there.

- If your domain has an SPF record, make sure it's up to date. It's not uncommon for organizations to create the SPF record and completely forget to update it as new IPs are added or removed. This is a vital fraud prevention measure. If your SPF record is not up to date, receiving mail servers may end up dropping perfectly good mail.
- Make sure you are not inadvertently breaking your DKIM signature. DKIM signatures can break if additional information is appended to the message once signed or if a public key is incorrect.
- If you have published your DMARC policy and it is not set to quarantine or reject, work aggressively to get to that stage. Your DMARC deployment won't benefit your customers until after you go beyond the “monitor phase.”
- Add additional layers to your phishing defense strategy—including global threat intelligence—for real-time updates on zero-day and zero-hour threats.

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. Technologies that offer protection both at the time a message is scanned at the gateway and when the message is clicked on by the user are also key components for a layered protection strategy. Core technologies like global threat intelligence that provide message reputation, file reputation, and sender reputation offer additional protection against known and emerging malware-based threats.

More Information
For more information on McAfee Email Protection, with its flexible deployment options—on-premises, Security-as-a-Service (SaaS), and an integrated hybrid solution—please visit: www.mcafee.com/emailsecurity.