

EMAIL AUTHENTICATION: A STEP BY STEP GUIDE

Tom Bartel | CIPP, Chief Privacy Officer | August 1, 2007

WHAT IS EMAIL AUTHENTICATION AND WHY IS IT IMPORTANT?

Authentication technology allows the receiver of an email and the Internet Service Provider (ISP) to confirm the identity of the sender. If the identity of the sender can not be authenticated, then ISPs may reject the message, or put it through additional filters to determine if it should be delivered. Without authentication, your chances of being filtered or blocked by major ISPs are greatly increased.

Email authentication is important because it addresses one of the fundamental security problems inherent to email sending technology. By exploiting such weaknesses spammers, phishers and spoofers have been able to thrive. Authentication is integral to preventing phishing and other fraud while playing a key role in the emerging reputation and accreditation systems that will drive the future of email. As a legitimate business, authentication is not optional; rather it is essential to securing your brand and online reputation. This paper provides guidelines and recommendations for legitimate businesses seeking to improve their deliverability rates and protect their brand from domain forgery and phishing scams.

HOW DOES AUTHENTICATION WORK?

ISPs are utilizing two primary methods of authentication: IP and cryptographic. The IP solution ties a responsible sending domain back to a set of permitted IP addresses, which requires publishing text (TXT) records in the Domain Name Service (DNS) record for each of your domains. Examples of an IP-based solution are SPF and Sender ID. Cryptographic authentication signs each message in a way that is difficult to forge, proving that the message came from the indicated sending domain. An example of a cryptographic approach is Yahoo! Domain Keys.

Today there is no single method accepted by all ISPs so businesses must comply with the authentication requirements set by the primary players. AOL uses Sender Policy Framework (SPF); Microsoft (Hotmail, MSN and Exchange) uses Sender ID; and Yahoo! requires Domain Keys. Most of the smaller ISPs are relying on some or all of these methods to authenticate email senders. In addition, businesses must broadly adopt authentication across all their domains, not just those associated with a large volume of commercial email. This includes domains used for corporate email, customer support and other services. While most online fraud is associated with high-profile marketing domains, without authentication it is possible for any of your domains to be spoofed – and for critical business functions to be compromised.

HOW DO I COMPLY WITH SPF & SENDER ID STANDARDS?

1 Provide your IT department with detailed information on the process

- Microsoft Sender ID: <http://www.microsoft.com/senderid>
- SPF Website: <http://www.openspf.org>

2 Identify the IP addresses your organization uses to send email

Take an inventory of all machines and systems that send email on behalf of your organization, including external systems such as Email Service Providers (ESPs) or other authorized 3rd parties.

Be sure to consider the following sources:

- Advertising/PR Agencies
- Corporate email
- Customer support and services
- Event marketing services
- Forwarding services
- Human resources
- Investor relations
- Newsletters
- Transactional email including order and shipping confirmations

3 Create your authentication records using the following tools and guides

- Microsoft Sender ID Framework Wizard:
<http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard>
- SPF Record Wizard: <http://www.openspf.org>
- Sender Score Certified SPF/Sender ID Deployment Guide
http://www.senderscore.com/pdf/ss_SPFSenderID.pdf

4 Publish your authentication records

With the assistance of the team responsible for managing DNS records for your domains, publish your email authentication records. The actual publishing of the records is straightforward; determining who controls your DNS records can be tricky but your IT department will be able to find out. In addition, some DNS providers cannot publish TXT in DNS.

A good resource on this topic is the Authentication and Online Trust Alliance, visit: http://aotalliance.org/docs/dns_txt_list.pdf for more information.

5 Validate your records

Confirm that your records are error-free. Here are some of the many testing options available:

- Return Path SPF – Sender ID testing tool: <http://senderid.returnpath.net>
- DNS Stuff SPF/Sender ID Testing Tool: <http://www.seoconsultants.com/tools/spf/>
- OpenSPF: <http://www.openspf.org/why.html>

6 Submit your domains to the Microsoft cache

You are encouraged to email Microsoft after you post your Sender ID or SPF record to the DNS, for complete information visit:

<http://www.microsoft.com/mscorp/safety/technologies/senderid/resouces>

7 Maintain valid authentication records

Be prepared to update records as your environment or the authentication landscape changes. Changes to your system (i.e. new domains or IP addresses) may require changes or additions to your record.

HOW DO I COMPLY WITH YAHOO! DOMAIN KEYS AND DOMAIN KEYS IDENTIFIED MAIL?

The process for complying with Yahoo! Domain Keys (DK) and Domain Keys Identified Mail (DKIM) will depend on your email infrastructure and you will need your IT department to be involved in the process. We recommend the following websites to learn more and determine next steps for your organization:

- <http://www.dkim.org/>
- <http://antispam.yahoo.com/domainkeys>

WILL AUTHENTICATION SOLVE MY DELIVERY PROBLEMS?

It's important to note that SPF, Sender ID and other authentication programs will not solve your deliverability problems. Validating a domain does not speak to the content or value of the message, only to the identity of the responsible sender. Authentication will make it harder for your domains to be forged and is critical to your deliverability since most ISPs make authentication a requirement for inclusion on a whitelist. However, authentication will not compensate for weak practices around content, permission standards, bounce handling, complaints or filter triggers.

Permission-based marketers must be vigilant and proactive managers of their deliverability status. First, monitor blocking, filtering and blacklisting by campaign, by ISP and by widely used corporate filters – and take proactive steps to correct any root causes of failure. Comply with all appropriate legislation. Ensure your sending infrastructure, permission policy and bounce handling procedures follow best practices. And, of course, monitor and respond to complaints and customer feedback.

If you have questions about authentication or would like to hear how Return Path's services can improve your email delivery and performance, please call 866-362-4577, or email rpinfo@returnpath.net.