

The Urgent Need to Implement E-Mail Authentication ***A value proposition for senders, users, and domain holders***

By Craig Spiegle
Director, Microsoft Technology Care and Safety

Spamming, spoofing, and phishing continue to undermine the integrity of e-mail as consumers begin to lose confidence in using e-mail and conducting business online. Last year the Pew Research Center reported that 63 percent of consumers trust e-mail less and 30 percent of users now use it less than the previous year. If the trends remain unchecked, they are likely to worsen with the rising epidemic of deceptive e-mail and online exploits.

Fortunately the industry is making headway through a combination of innovative technologies that provide prescriptive guidance, effective legislation and enforcement, and industry collaboration. The most promising effort to date—one that is demonstrating real results—is e-mail authentication.

This article outlines new approaches and prescriptive help for preserving e-mail integrity:

- What are spamming, spoofing, and phishing?
- What's new in e-mail authentication?
- What is Sender ID?
- How does Sender ID work?
- How do we implement Sender ID?
- How can we learn more?

What are spamming, spoofing, and phishing?

Spamming is the sending of unsolicited commercial e-mail—also known as junk e-mail. *Spoofing* is the common practice of altering the “From” address of an e-mail so that it appears to come from a legitimate sender. *Phishing* is the attempt to trick e-mail recipients into giving out personal information, such as credit card numbers or account passwords, by sending e-mail pretending to be from a legitimate source, such as a user's bank, credit card company, or online Web merchant. Most phishing attacks come from e-mail in which the senders name in the “from line” has been forged or spoofed.

What's new in e-mail authentication?

Over the past 18 months, authenticated mail has evolved significantly from concept discussions and debate, to actual implementation. Two primary approaches have emerged. The Sender ID Framework (SIDF) is an Internet Protocol (IP)–based solution that developed from the merger of two proposals: Sender Policy Framework (SPF) and the Microsoft Caller ID for E-mail. Complementing SIDF is the emerging signing proposal called DKIM which combines Yahoo! DomainKeys and Cisco's Identified Internet Mail (IIM) specifications. Of these solutions, Sender ID, utilizing the SPF record format is now being implemented worldwide, is royalty free, and is easy to implement by both Internet service providers (ISPs) and business email environments of all sizes.

Today, industry e-mail leaders, such as MSN Hotmail, and more than 1.2 million domains have realized the promise of IP-based solutions by publishing SPF records and completing the Sender ID check. Early implementation benefits include improved spam detection, enhanced sender reputation scoring, and have provided a reduction in false-positive incidents among Sender ID–compliant mail senders.

What is Sender ID?

SIDF helps protect against e-mail domain spoofing and provides greater protection against phishing schemes. Sender ID checks and validates the sending server's IP address(s) to verify the sending domain is authorized to send mail on its behalf. Reducing domain spoofing helps legitimate senders protect their domain names and reputations, and helps recipients more effectively identify and filter junk e-mail and phishing exploits.

Sender ID provides the choice of checking of the SPF record using one of two check mechanisms: the Purported Responsible Address (PRA) or the "Mail From". When checking the validity of the SPF record using either of them and incorporating the result with your existing anti-spam heuristics, you can help improve e-mail deliverability, reduce spam and reduce false positives.

How does Sender ID work?

Your domain administrator or hosting company simply publishes SPF records in the Domain Name System (DNS). These simple text records identify authorized outbound e-mail servers by listing their IP addresses. Receiving e-mail systems verify if messages originate from properly authorized outbound e-mail servers. The steps are:

1. The sender transmits an e-mail message to the receiver.
2. The inbound mail server receives the e-mail and does the following:
 - Checks which domain claims to have sent the message and checks DNS for the SPF record of that domain.
 - Determines if the sending server's IP address matches any of the IP addresses that are published in the SPF record.
 - Scores the e-mail: If the IP addresses match, the mail is authenticated and receives a positive score. If the addresses do not match, the mail fails authentication and receives a negative score. These results are then applied to existing anti-spam filtering policies and heuristics.

How do we implement Sender ID?

To implement Sender ID, you first need to create and publish your SPF record, which is a complete inventory of all the IP addresses that your domain uses to send mail. Be sure to include the IP addresses of any third parties who send mail for you.

Visit the cross-industry Web site, www.emailauthentication.org/resources.html, which provides e-mail authentication tools and other resources to assist the IT and business communities. On this site you can also access the Sender ID Framework SPF Record which provides a step-by-step process to create your SPF record. Using this tool, you can complete an automated inventory of your domain's published IP addresses and create your record.

How can we learn more?

Because of the significant, long-term benefits in implementing authentication solutions, an industry coalition of more than three dozen companies, have organized the Email Authentication Implementation Summit 2005. Being held on July 12, 2005, in New York City, this event sets the stage at the broadest industry level to help ensure the integrity and reputation of legitimate e-mail.

Moderated by Esther Dyson, editor for Release 1.0 at CNET Networks, attendees of this full day program will learn from leading experts in safety and online security including Cisco, IronPort, Microsoft, MSN Hotmail, Sendmail, Symantec, Tumbleweed and Yahoo! as they share best practices from working with leading eCommerce sites and financial institutions including eBay, Amazon, Bank of America and Paypal. In addition, marketing and brand executives will learn from the DMA, ESPC, Bigfoot Interactive, Digital Impact and DoubleClick and others on how domain holders can join in the fight against spam and phishing. The event includes breakout sessions designed for IT professionals, business decision makers and e-mail marketing executives, providing actionable and prescriptive information. To attend, visit www.emailauthentication.org/summit2005 and register today!