

# Sender Policy Framework Not Effective Against Spam

*LinuxReviews.org*

Sender Policy Framework (SPF) is a new e-mail authentication protocol meant to stop spam-mail. Statistics from CipherTrust show SPF is working against its intention because spam-senders are much quicker than legitimate ISPs to adopt the standard.

The result is that e-mail servers who accept or reject e-mails based on the Sender Policy Framework (SPF) rules are more likely to stop important e-mails sent from valid, legitimate mail-servers who have not implemented the standard while spam-mail are likely to pass through because spam-senders are the first to adapt any rule aimed at stopping them.

CipherTrust research recently analyzed e-mail messages from over 1000 enterprises worldwide and found that **34 percent more spam** passes the SPF checks than real, legitimate e-mail. The chances of a spam-message being legitimated by SPF checks is three times higher than the chance of the checks stopping it.

SPF checks if the Internet address trying to send a message belongs to the domain which claims to be sending the message. This is done by checking if the IP address has a reverse MX DNS record with that domain. This is why many legitimate e-mail users ignore the standard: It is not standard to have complete control over the reverse records of your IPv4 IP or subnet, chances are high you require your ISP to change or add such records. The modern Internet standard, IPv6, has a bigger address space and a IPv6 user is much more likely than a IPv4 to control reverse delegations, but as with IPv4 being able to set your reverse records is a luxury, not a standard.

Linux users have long benefited from how easy it is to get a working mail system with virtual domains and advanced spam filtering using standard software building blocks like postfix, courier-imap amavisd and Spamassassin. Mail from a typical Linux user running his own personal mail system are likely to be identified as spam by SPF checks, simply because home ADSL users have no control what so ever over their reverse DNS records.

Spam-senders do make money off their various scams and direct much more time, effort and attention towards being able to mass-mail messages than your average ISP who has had a working mail system for years.

**SPF is not a official standard, more a recommendation. Our recommendation: Don't use it, your chances of stopping important messages by implementing it are higher than your chances of receiving less spam.**

---

> [Linux Reviews](#) > [News and headlines](#) > [2004 News archive](#) > [September](#)

>

Sender Policy Framework Not Effective Against Spam