

Defense against spam

DKIM

DKIM (DomainKeys Identified Mail) is a cryptographic method for signing mail. Mail is signed with the private key on the mail server. The public key may be retrieved from the domains TXT record for verification.

SPF

WORKING

The SMTP protocol was not originally designed to be very resistant to spoofing. SPF tries to help by reading rules about sender servers from the domain TXT records.

PROBLEMS

SPF does not take redirected mail into account. Due to SPF, all redirected mail would be discarded as fake.

RECOMMENDATION

Don't use SPF. Instead, use DKIM.

Further reading:

[Wikipedia](#)

[Why you shouldn't jump on the SPF bandwagon](#)

[Sender Policy Framework project](#)

DCC

DCC (Distributed Checksum Clearinghouses) creates a checksum from all mail. If the same checksum is detected many times, the spam score is increased.

PYZOR

Pyzor is an offspring of Razor and works in a similar manner. Mail checksums are collected and checked against multiple rules on central servers.

RAZOR

Razor is a closed source community spam filter. Further reading: [Vipul's Razor](#)

Revision #1

Created 25 October 2023 12:58:48 by Judit Pásztor

Updated 25 October 2023 12:59:14 by Judit Pásztor