SPF (Sender Policy Framework)

Introduction

> Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of the email. SPF alone, though, is limited only to detect a forged sender claimed in the envelope of the email which is used when the mail gets bounced. Only in combination with DMARC can it be used to detect the forging of the visible sender in emails (email spoofing), a technique often used in phishing and email spam. source

Description

SPF is the most basic email authentication method. It involves simple DNS records that allow you to specify what servers email can originate from for the domain specified in the email envelope.

Read More

Example

As an example, `swigg.net` is setup with two SPF rules.

Domain	Type	Value
@	TXT	v=spf1 mx include:_spf.google.com include:me.com -all
*	TXT	v=spf1 mx:swigg.net -all

These two entries can be read as follows:

1. Any email ending in `@swigg.net` has to originate from one of the MX records defined for swigg.net **or** from a Google/Apple server defined in *their* SPF policy. Any other server

sending email on behalf of this domain will be rejected.
2. Any email ending in `@*.swigg.net` has to originate from one of the MX records defined for swigg.net. Any other server sending email on behalf of these domains will be rejected.

Revision #6
Created 29 October 2020 16:57:40 by dustin@swigg.net
Updated 29 October 2020 18:28:11 by dustin@swigg.net