POWERDMARC

Datasheet

# Take Control of Your Domain With SPF

The biggest threat to your customer's email security is an attacker using your brand name and domain to send fake messages. **Phishing emails** like these can be convincing enough that your customers won't know the difference — and end up falling prey to a scam. This can **damage both your brand image and your reputation** with email providers, making it less likely that your actual emails reach customer inboxes.

## Block Out Unauthorized Senders

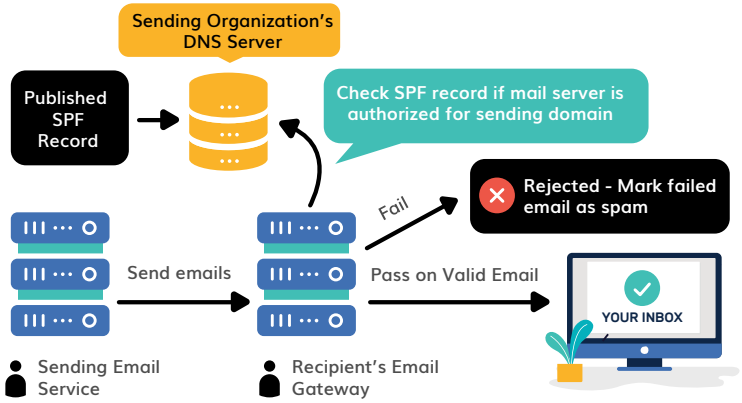
Sender Policy Framework, or SPF, is one of the earliest and most widely used industry standards for email security. It operates on a simple concept: only allow explicitly authorized senders to send emails from your domain, and block everyone else. When you implement SPF on your domain, here's what happens:

### Publish SPF Records

You must publish SPF records on your DNS, containing a list of all approved IP addresses that can send emails.

### Email Server Authentication

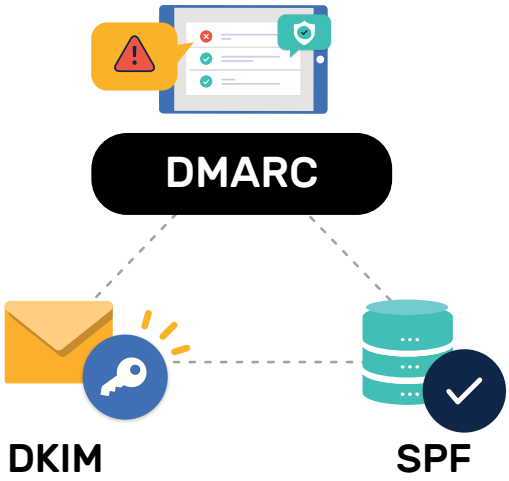
When a receiving email server sees an email from your domain, it crosschecks the sender's IP address with the list you provided.




If the sender's IP matches one on the list, it gets authenticated and is sent to the destination inbox. If it doesn't match, the email fails authentication and gets rejected by the server.

# Make SPF Even Better With PowerDMARC

SPF by itself is still effective, but cybercriminals have come up with ways to bypass the IP address verification phase. But SPF technology is made relevant again by incorporating it into DMARC. What are the benefits of doing this? We'll tell you:




## SPF + DKIM = DMARC

DMARC uses both SPF and DKIM (DomainKeys Identified Mail) technologies in tandem to give your domain even better protection against spoofing. PowerDMARC takes this one step further with AI-based real-time threat modeling that uncovers spoofing attacks around the globe.

## Reporting & Feedback With PowerDMARC

Neither SPF nor DKIM give the domain owner feedback about emails that fail authentication. DMARC sends detailed reports directly to you, which the PowerDMARC app converts into easy-to-read charts and tables. Using the analytics data, you can change your email marketing strategy on the fly.

## Control What Happens to Unauthenticated Email

DMARC lets you, the domain owner, decide whether email that fails validation goes to inbox, spam or gets rejected. With PowerDMARC, all you have to do is click one button to set your DMARC policy. It's that easy.

SPF used to be the best in email security, but it just got WAY better with DMARC. Get your domain fortified with PowerDMARC now!