SYSTEMAGIC
DOING IT DIFFERENTLY

# WHY DKIM AND SPF RECORDS ARE IMPORTANT

## What is DKIM?

DKIM (DomainKeys Identified Mail) is a security feature designed to protect your email communications. It works by adding a digital signature to your emails, which serves as proof that the email was sent from your domain and hasn't been tampered with during transit.

Think of DKIM as a seal on a letter. If the seal is intact when the recipient receives the letter, they can be confident that the message inside hasn't been altered. This ensures that the emails you send are authentic and trustworthy.

## What About SPF?

SPF (Sender Policy Framework) is another security tool that helps prevent email spoofing. Spoofing is when someone sends an email pretending to be from your domain. SPF combats this by allowing you to specify which mail servers are authorised to send emails on behalf of your domain. It's like creating a guest list for a party—only those on the list are allowed to enter.

## Why Are DKIM & SPF Important?

DKIM and SPF are crucial for maintaining your domain's reputation and ensuring that your emails reach their intended recipients.

Without these records in place, scammers and cybercriminals can easily send emails that appear to be from your domain, potentially leading to a loss of trust in your brand.

For example, if someone receives a phishing email that looks like it came from your company, they might be hesitant to open future emails from you, even if they're legitimate.

This can damage your reputation and lead to a decline in customer confidence.

Channel Futures. Leading Channel Partners Forward
MSP 501
2022 WINNER

Microsoft Solutions Partner
Modern Work

Certified Mac Technician

CYBER ESSENTIALS PLUS

# IMPROVED DELIVERABILITY

In addition to protecting your reputation, DKIM and SPF play a significant role in improving email deliverability. Many email providers, such as Gmail, Outlook, and Yahoo, check for DKIM and SPF records before deciding whether to deliver an email to the inbox or the spam folder.

If your emails lack these records, they might be marked as spam, even if they are perfectly legitimate. By setting up DKIM and SPF, you can help ensure that your emails land where they're supposed to—in your recipients' inboxes.

## The Bottom Line

DKIM and SPF records are essential tools for protecting your domain and ensuring that your emails are delivered correctly.

By setting them up, you can safeguard your brand's reputation, improve email deliverability, and prevent phishing and spoofing attacks.

Taking the time to configure these records is a small investment that can pay big dividends in terms of security and customer trust.

## PROTECT YOUR INBOX AND IMPROVE DELIVERABILITY


01225 426800

info@systemagic.co.uk

www.systemagic.co.uk


