Somerbys IT

Email Authentication

A Simple Guide for Business Owners

Introduction

Email authentication is essential for protecting your business from email-based threats like phishing and spoofing. It involves three main protocols: SPF, DKIM, and DMARC. These protocols help verify that the emails you send are genuine and not forged by malicious actors.

1. SPF (Sender Policy Framework)

What is SPF?
SPF is a protocol that allows you to specify which mail servers are allowed to send emails on behalf of your domain. It helps to prevent unauthorised people from sending emails pretending to be from your domain.

How Does SPF Work?

- You create an SPF record in your domain's DNS settings.
- This record lists the IP addresses of servers that are authorised to send emails for your domain.
- When an email is received, the recipient's mail server checks the SPF record to verify if the email is coming from an authorised server.

Why is SPF Important?

- **Prevents Email Spoofing:** Stops spammers from using your domain to send fake emails.
- **Protects Brand Reputation:** Ensures your customers trust that emails from your domain are legitimate.
- **Improves Email Deliverability:** Authenticated emails are less likely to be marked as spam.

92%

of organisations were victims of phishing attacks in 2023

DMARC report, 2023

2. DKIM (DomainKeys Identified Mail)

What is DKIM?
DKIM adds a digital signature to your emails, which helps recipients verify that the emails are indeed from you and have not been altered in transit.

How Does DKIM Work?

- You generate a pair of cryptographic keys: a private key and a public key.
- The private key is used to sign your emails.
- The public key is published in your domain's DNS.
- When an email is received, the recipient's mail server uses the public key to verify the signature.

Why is DKIM Important?

- **Ensures Email Integrity:** Confirms that the content of the email has not been tampered with.
- **Authenticates Sender Identity:** Proves that the email is genuinely from your domain.
- **Boosts Trust:** Recipients are more likely to trust and open your emails.

3. DMARC (Domain-based Message Authentication, Reporting & Conformance)

What is DMARC?
DMARC builds on SPF and DKIM by adding a policy layer, allowing you to specify how your emails should be handled if they fail SPF or DKIM checks. It also provides a reporting mechanism.

How Does DMARC Work?

- You create a DMARC record in your domain's DNS.
- This record tells receiving mail servers what to do if an email fails SPF or DKIM checks (e.g., reject, quarantine, or do nothing).
- It also provides an email address where you can receive reports on the authentication results.

Why is DMARC Important?

- **Enhanced Protection:** Enforces your email authentication policies to prevent unauthorised use of your domain.
- **Visibility and Reporting:** Gives you insights into who is sending emails on behalf of your domain and the authentication results.
- **Trust and Security:** Helps to secure your email communications, making your domain more trustworthy.

Why Email Authentication Matters for Your Business

1. Prevent Phishing and Fraud: By using SPF, DKIM, and DMARC, you make it much harder for attackers to send fake emails pretending to be from your business.

2. Protect Your Brand: Unauthorised use of your domain can damage your reputation. Email authentication helps protect your brand integrity.

3. Improve Email Deliverability: Authenticated emails are more likely to reach your customers' inboxes rather than being marked as spam.

4. Gain Insights: DMARC reports provide valuable information about email traffic using your domain, helping you identify potential abuse and improve security measures.

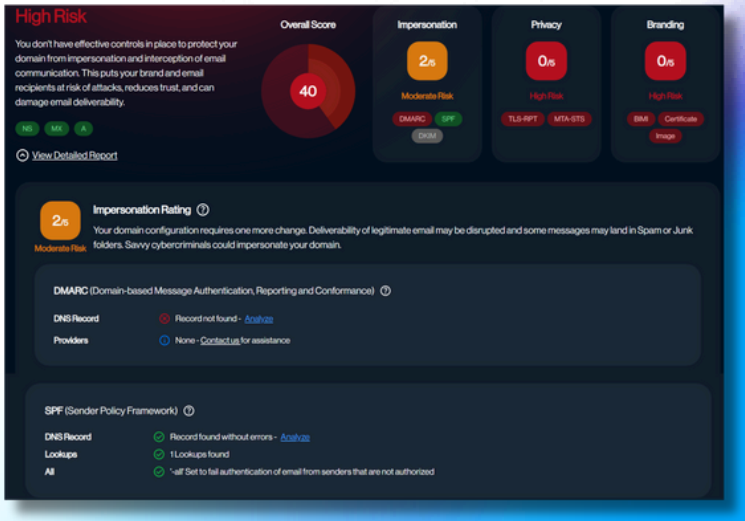
Getting Started

1. Set Up SPF: Add an SPF record to your domain's DNS. List the IP addresses of authorised mail servers.

2. Implement DKIM: Generate DKIM keys and add the public key to your DNS. Configure your email server to sign outgoing emails with the private key.

3. Deploy DMARC: Create a DMARC record in your DNS. Specify the policy for handling failed emails and provide an email address for reports.

By implementing these protocols, you can secure your email communications and protect your business from email-based threats.



Concerned about your email security?

At Somerbys IT, we offer a thorough analysis of your email security and provide a detailed report.

Conclusion

Email authentication with SPF, DKIM, and DMARC is a powerful way to safeguard your business's email communication. It helps protect against fraud, maintain your brand's reputation, and ensure that your emails reach your customers. Take the steps to implement these protocols and enhance your email security today.

We hope you've found this guide useful.

If you're concerned about your email security, we can help. Get in touch with the experts at Somerbys IT.

0333 456 4431 | info@somerbysit.co.uk

The Dock
75 Exploration
Drive Leicester,
LE4 5NU

Somerbys IT