ACTIVELY BLOCK PHISHING ATTACKS AND INCREASE EMAIL DELIVERABILITY WITH DMARC

Phishing attacks are one of the most sophisticated, common, and damaging incidents a business will face.

96%

On average, 96% of cyberattacks start with a phishing email[1]

$4.65M

The average cost of a breach through phishing is $4.65 million[2]

-5%

Organizations see a 5% drop in stock price in the first 6 months following a breach[1]

To protect themselves from phishing and BEC attacks, organizations must adopt a multi-layered cyber strategy. The DMARC protocol is an essential part of this approach.

What is DMARC?

DMARC, which stands for *Domain-based Message Authentication, Reporting & Conformance*, is an email authentication protocol which stops schemers from being able to use your domain to send fraudulent emails to your employees and customers. It builds on the SPF and DKIM protocols, adding a reporting and enforcement function that allows senders to block fraudulent email that uses their domain and increase deliverability.

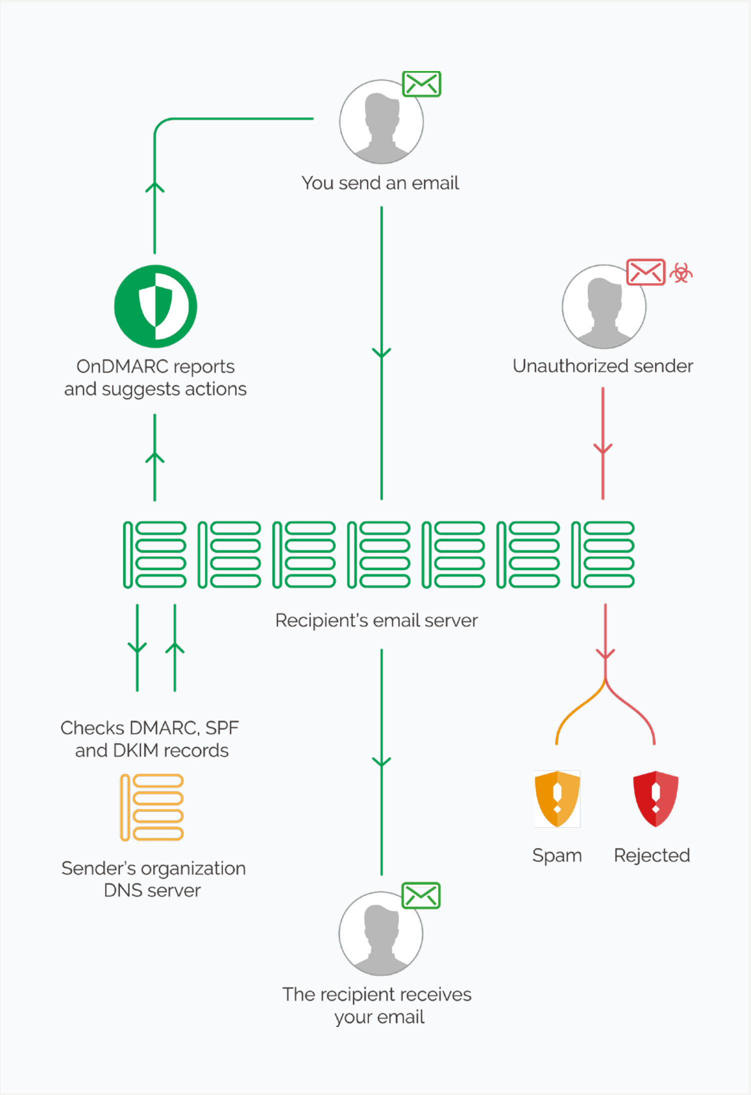
SPF

Sender Policy Framework is a protocol that validates if a server is authorized to send emails on behalf of a domain.

DKIM

DomainKeys Identified Mail is a digital signature that confirms that the email content has not been tampered with.

DMARC uses the validation results of SPF & DKIM to understand if the email is authorized by the domain owner. Using this validation, it can tell receiving servers to reject or quarantine such email.


You send an email
OnDMARC reports and suggests actions
Unauthorized sender
Recipient's email server
Checks DMARC, SPF and DKIM records
Sender's organization DNS server
Spam
Rejected
The recipient receives your email

[1] *Verizon 2021 Data Breach Investigations Report*
[2] *IBM Cost of a Data Breach Report 2021*

Ready to secure your organization's email inboxes against phishing?

CONTACT US

The solution: OnDMARC

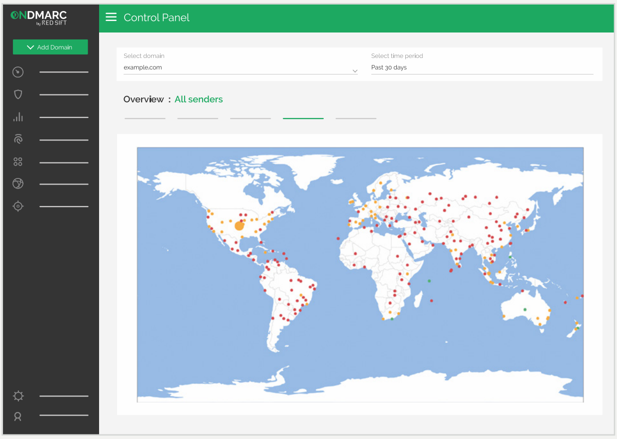
With OnDMARC, you can block damaging emails from going straight to your customers, suppliers, and other key contacts by getting your DMARC policy to p=reject quickly and effectively. When you have this policy in place your sender reputation also improves, increasing deliverability and avoiding costly diversions to spam.

Our DMARC based protection solution focuses on:

- ✓ Safe, quick implementation of the DMARC protocol to protection mode, usually completed in an average 4-8 week timeframe
- ✓ Managing your DMARC, SPF, DKIM and BIMI records directly from OnDMARC
- ✓ Automation of SPF records and the secure removal of the 10 lookup limit currently inherent in the SPF protocol
- ✓ Providing the support required to reach protection (or p=reject), alongside ongoing maintenance and reporting
- ✓ Protection of all the domains you own, including any which are not currently configured to send email

ONDMARC by RED SIFT

Block phishing attacks and increase email deliverability



Select domain: example.com

Select time period: Past 30 days

Overview : All senders

OnDMARC's key benefits

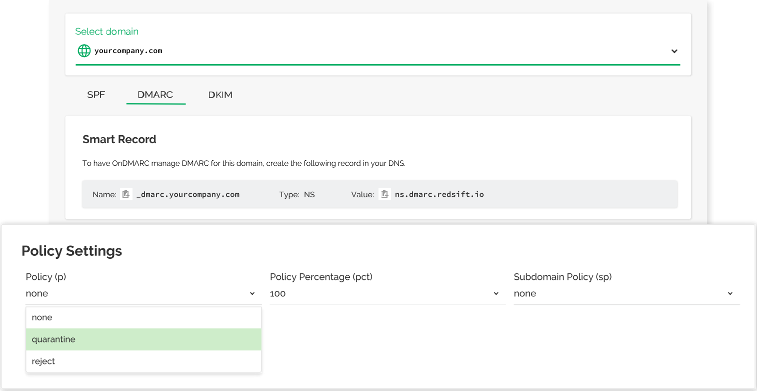
- Ensure financial security
- Secure the supply chain
- Improve email deliverability
- Stop Business Email Compromise
- Identify and remove shadow IT
- Comply with GDPR

Why do organizations choose OnDMARC?

OnDMARC lets you fast-track your journey to full protection with unique features such as:

Dynamic DMARC

Dynamic DMARC enables the management of DMARC, DKIM, SPF, BIMI, and MTA/STS TXT records from within OnDMARC. This means that once the OnDMARC Smart Records have been added to a domain's DNS via our simple interface, there's no need to go back to the DNS since all your records are now automatically updated.



Select domain: yourcompany.com

Smart Record

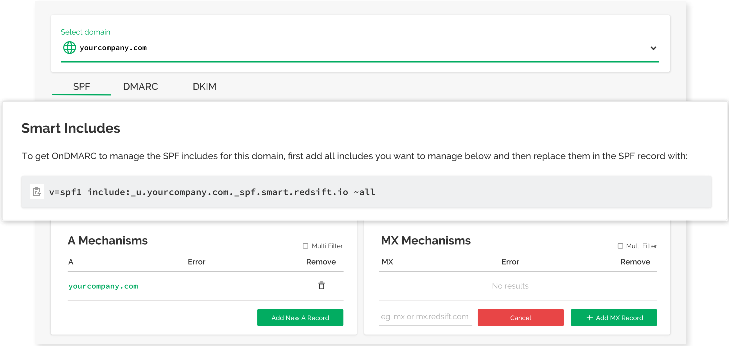
To have OnDMARC manage DMARC for this domain, create the following record in your DNS.

Name: `_dmarc.yourcompany.com` Type: NS Value: `ns.dmarc.redsift.io`

Policy Settings

Policy (p)	Policy Percentage (pct)	Subdomain Policy (sp)
none	100	none

none
quarantine
reject



Select domain: yourcompany.com

Smart Includes

To get OnDMARC to manage the SPF includes for this domain, first add all includes you want to manage below and then replace them in the SPF record with:

```
v=spf1 include:_u.yourcompany.com._spf.smart.redsift.io ~all
```

A Mechanisms □ Multi Filter

A	Error	Remove
yourcompany.com		

MX Mechanisms □ Multi Filter

MX	Error	Remove
No results		

eg. mx or mx.redsift.com

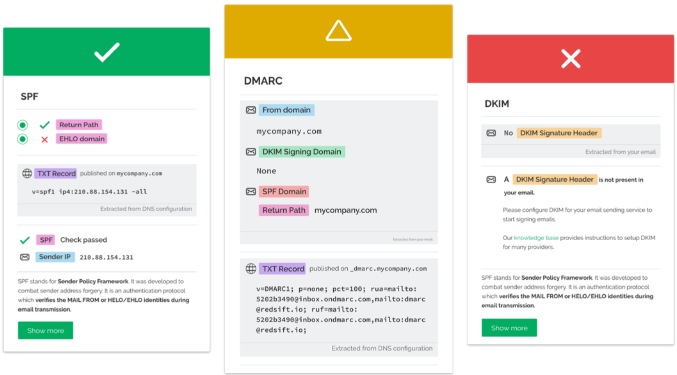
Dynamic SPF

Dynamic SPF allows you to overcome the 10 lookup limit by using a single dynamic include to combine all authorized services correctly at the point of query. This prevents your authorized traffic from failing SPF validation and means your organization's email deliverability will never be impacted.

Ready to secure your organization's email inboxes against phishing? CONTACT US RED SIFT

Investigate

With a feature like *Investigate*, you hold the key to quickly unlocking the information hidden in email headers and turning it into something you can easily work with for perfect DMARC configuration. You can instantly see the results of every change you made to your email security with a fast automated checklist via *Investigate*'s inbox in your OnDMARC account.



✓

SPF

● ✓ Return Path
● ✕ EHLO domain

TXT Record published on mycompany.com

```
v=spf1 ip4:210.88.154.131 ~all
```

Extracted from DNS configuration

✓ SPF Check passed

Sender IP 210.88.154.131

SPF stands for **Sender Policy Framework**. It was developed to combat sender address forgery. It is an authentication protocol which **verifies the MAIL FROM or HELO/EHLO identities during email transmission.**

△

DMARC

From domain

mycompany.com

DKIM Signing Domain

None

SPF Domain

Return Path mycompany.com

Extracted from your email

TXT Record published on _dmarc.mycompany.com

```
v=DMARC1; p=none; pct=100; rua=mailto:
5202b3490@inbox.ondmarc.com,mailto:dmarc
@redsift.io; ruf=mailto:
5202b3490@inbox.ondmarc.com,mailto:dmarc
@redsift.io;
```

Extracted from DNS configuration

✕

DKIM

No DKIM Signature Header

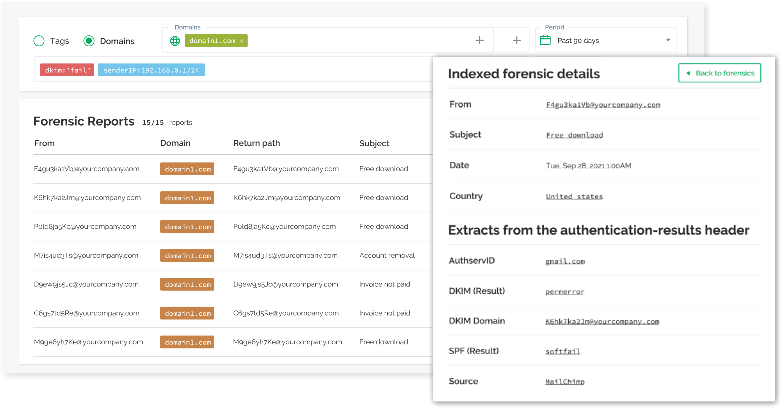
Extracted from your email

A DKIM Signature Header **is not present in your email.**

Please configure DKIM for your email sending service to start signing emails.

Our knowledge base provides instructions to setup DKIM for many providers.

SPF stands for **Sender Policy Framework**. It was developed to combat sender address forgery. It is an authentication protocol which **verifies the MAIL FROM or HELO/EHLO identities during email transmission.**



○ Tags ● Domains

Domains: domain1.com ×

Period: Past 90 days

dkim:'fail' senderIP:192.168.0.1/24

Forensic Reports 15/15 reports

From	Domain	Return path	Subject
F4gu3ka1Vb@yourcompany.com	domain1.com	F4gu3ka1Vb@yourcompany.com	Free download
K6hk7ka2Jm@yourcompany.com	domain1.com	K6hk7ka2Jm@yourcompany.com	Free download
P0ld8ja5Kc@yourcompany.com	domain1.com	P0ld8ja5Kc@yourcompany.com	Free download
M7is4ud3Ts@yourcompany.com	domain1.com	M7is4ud3Ts@yourcompany.com	Account removal
D9ewgjs5Jc@yourcompany.com	domain1.com	D9ewgjs5Jc@yourcompany.com	Invoice not paid
C6gs7td5Re@yourcompany.com	domain1.com	C6gs7td5Re@yourcompany.com	Invoice not paid
M9ge6yh7Ke@yourcompany.com	domain1.com	M9ge6yh7Ke@yourcompany.com	Free download

Indexed forensic details

From	F4gu3ka1Vb@yourcompany.com
Subject	Free download
Date	Tue, Sep 28, 2021 1:00AM
Country	United states

Extracts from the authentication-results header

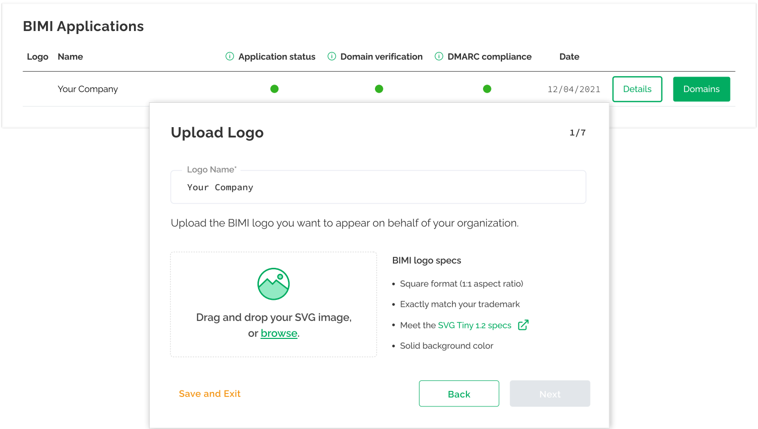
AuthservID	gmail.com
DKIM (Result)	permerror
DKIM Domain	K6hk7ka2Jm@yourcompany.com
SPF (Result)	softfail
Source	MailChimp

Sender Intelligence

Imagine DMARC reports that work harder for you - that's what *Sender Intelligence* provides. A new kind of forensic reporting that contextualizes the relevant and granular information about your sending sources, enabling you to pinpoint and solve issues within your organization quickly

BIMI

Increase brand recall, improve email open rates, and influence buyer behavior by putting your trademarked logo next to every email you send with the only integrated BIMI and VMC integration available on the market.



BIMI Applications

Logo	Name	Application status	Domain verification	DMARC compliance	Date		
	Your Company	●	●	●	12/04/2021	Details	Domains

Upload Logo 1/7

Logo Name*: Your Company

Upload the BIMI logo you want to appear on behalf of your organization.

Drag and drop your SVG image, or browse.

BIMI logo specs

- Square format (1:1 aspect ratio)
- Exactly match your trademark
- Meet the SVG Tiny 1.2 specs
- Solid background color

Find out how you can use OnDMARC to combat phishing and boost email deliverability.

START YOUR FREE TRIAL

BRITISH LEGAL TECHNOLOGY Awards 2020 WINNER FOR 'IT SECURITY PROVIDER OF THE YEAR'

Member of Microsoft Intelligent Security Association Microsoft

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2021

SecurityScorecard

2021 FORTRESS CYBER SECURITY AWARD

bsi. ISO/IEC 27001 Information Security Management IS 672913

THE CHANNEL CO. CRN EMERGING VENDORS 2021

RED SIFT

Founded in 2015, Red Sift is a global cybersecurity company whose clients include organizations such as Domino's, Telefonica, Pipedrive, Rentokil, Wise, and top global law firms.

Products on the Red Sift platform work together to close the net on the phishing problem by blocking outbound phishing attacks, analyzing the security of inbound communications, and providing domain impersonation defense for company-wide threat protection.

redsift.com
contact@redsift.com
@redsift