



Missing DMARC Records Leading to Email Spoofing



Pending Fix

● LOW

• Reported by [fluhar](#) on May 18, 2025 • #PT30497_4

Vulnerability Type

Server Security Misconfiguration > Mail Server Misconfiguration > Email Spoofing to Inbox due to Missing or Misconfigured DMARC on Email Domain

Description

During the assessment, it was observed that the applications domains lack a DMARC record in their DNS configuration. This makes it easier for attackers to send spoofed emails using the organization's domain, which can deceive recipients and bypass basic spam filters.

DMARC is an email authentication protocol that builds on SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) to give domain owners control over how their email is handled if it fails authentication. A properly configured DMARC policy allows domain owners to instruct email providers to reject or quarantine unauthenticated messages and receive reports on email activity.

Affected Targets

<https://slkohlercampaign.com/>

<https://npkohlercampaign.com/>

<https://bdkohlercampaign.com/>

<https://bhkohlercampaign.com/>

OWASP Severity

● LOW



CVSS v3.1 Score

● LOW (3.1)

Proof of Concept

Step 1: Navigate to <https://mxtoolbox.com/dmarc.aspx> and enter the following domains.

- slkohlercampaign.com
- npkohlercampaign.com
- bdkohlercampaign.com
- bhkohlercampaign.com

Step 2: Observe that the DMARC record is not configured for the domains.

mxtoolbox.com/SuperTool.aspx?action=dmarc%3aslkohlercampaign.com&run=toolpage

MX TOOLBOX[®]
SUPERTOOL

Pricing Tools Delivery Center Monitorin

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers

SuperTool Beta9

slkohlercampaign.com DMARC Lookup

dmarc:slkohlercampaign.com Find Problems Solve Email Delivery Problems dmarc

	Test	Result	
+	DMARC Record Published	No DMARC Record found	More Info

Your DNS hosting provider is "GoDaddy" Need Bulk Dns Provider Data?

[dns lookup](#) [dns check](#) [mx lookup](#) [spf lookup](#) [dns propagation](#) [Transcript](#)

Reported by ns29.domaincontrol.com on 5/18/2025 at 3:05:27 AM (UTC -5), just for you.

ABOUT THE SUPERTOOL!

All of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool. Input a **domain name** or **IP Address** or **Host Name**. Links in the results will guide you to other relevant tools and information. And you'll have a chronological history of your results.

If you already know exactly what you want, you can force a particular test or lookup. Try some of these examples:

(e.g. "blacklist: 127.0.0.2" will do a blacklist lookup)

mxtoolbox.com/SuperTool.aspx?action=dmarc%3aslkohlercampaign.com&run=toolpage#

MX

TOOLBOX

SUPERTOOL

PricingToolsDelivery CenterMonitoring

SuperToolMX LookupBlacklistsDMARCDiagnosticsEmail HealthDNS LookupAnalyze Headers

SuperTool Beta9

npkohlercampaign.com

DMARC Lookup

dmarc:npkohlercampaign.com

Find Problems

Solve Email Delivery Problems

dmarc

Microsoft Outlook.com now requires DMARC - Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center

Test	Result	
<div>✖</div> DMARC Record Published	No DMARC Record found	<div>More Info</div>

Your DNS hosting provider is "GoDaddy" Need Bulk Dns Provider Data?

dns lookup

dns check

mx lookup

spf lookup

dns propagation

Reported by ns29.domaincontrol.com on 5/18/2025 at 3:10:10 AM (UTC -5), just for you.

Transcript

mxtoolbox.com/SuperTool.aspx?action=dmarc%3aslkohlercampaign.com&run=toolpage#

MX

TOOLBOX

SUPERTOOL

PricingToolsDelivery CenterMonitoring

SuperToolMX LookupBlacklistsDMARCDiagnosticsEmail HealthDNS LookupAnalyze Headers

SuperTool Beta9

bdkohlercampaign.com

DMARC Lookup

dmarc:bdkohlercampaign.com

Find Problems

Solve Email Delivery Problems

dmarc

Microsoft Outlook.com now requires DMARC - Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center

Test	Result	
<div>✖</div> DMARC Record Published	No DMARC Record found	<div>More Info</div>

Your DNS hosting provider is "GoDaddy" Need Bulk Dns Provider Data?

dns lookup

dns check

mx lookup

spf lookup

dns propagation

Reported by ns78.domaincontrol.com on 5/18/2025 at 3:11:07 AM (UTC -5), just for you.

Transcript

mxtoolbox.com/SuperTool.aspx?action=dmarc%3aslkohlercampaign.com&run=toolpage#

MX

TOOLBOX

SUPERTOOL

PricingToolsDelivery CenterMonitoring

SuperToolMX LookupBlacklistsDMARCDiagnosticsEmail HealthDNS LookupAnalyze Headers

SuperTool Beta9

bhkohlercampaign.com

DMARC Lookup

dmarc:bhkohlercampaign.com

Find Problems

Solve Email Delivery Problems

dmarc

Microsoft Outlook.com now requires DMARC - Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center

Test	Result	
<div>✖</div> DMARC Record Published	No DMARC Record found	<div>More Info</div>

Your DNS hosting provider is "GoDaddy" Need Bulk Dns Provider Data?

dns lookup

dns check

mx lookup

spf lookup

dns propagation

Reported by ns57.domaincontrol.com on 5/18/2025 at 3:12:02 AM (UTC -5), just for you.

Transcript

Impact

The absence of a DMARC record exposes the domain to email spoofing, which can be leveraged in phishing or social engineering attacks. While this does not directly compromise internal systems, it can significantly damage the organization's reputation, erode user trust, and increase the success rate of email-based threats. The risk becomes more critical if the domain is used for customer communication, invoicing, or internal operations.

Suggested Fix

SPF is not a sufficient email spoofing protection in case of some of the largest email providers. Emails spoofed for domains having properly configured hard fail SPF records may still be delivered to the recipient's inbox. In order to fully prevent email spoofing create a DMARC record with `~all=reject` policy. Please note that if your DMARC policy is not set up properly it may result in email delivery issues.

ACTIVITY

fluhar changed state to **Pending Fix**

May 18