

Hotmail email delivery fails after Microsoft misconfigures DNS

By [Lawrence Abrams](#)



August 18, 2023



11:44 AM



1



Hotmail users worldwide have problems sending emails, with messages flagged as spam or not delivered after Microsoft misconfigured the domain's DNS SPF record.

The email issues began late last night, with users and admins reporting on Reddit, Twitter, and Microsoft forums that their Hotmail emails were failing due to SPF validation errors.

A Hotmail user explained in a post on [Microsoft's forum](#) that their Microsoft Outlook Hotmail accounts were failing to send with the following error:

"For Email Administrators

This error is related to the Sender Policy Framework (SPF). The destination email system's evaluation of the SPF record for the message resulted in an error. Please work with your domain registrar to ensure your SPF records are correctly configured.

exhprdmxe26 gave this error:

Message rejected due to SPF policy - Please check policy for hotmail.com"

The Sender Policy Framework (SPF) is an email security feature that reduces spam and prevents threat actors from spoofing domains in phishing attacks.

To configure SPF, admins create a special DNS TXT (text) record for a domain that specifies the specific hostnames and IP addresses allowed to send emails under that domain.

When a mail server receives an email, it will verify that the hostname/IP address for the sending email servers is part of a domain's SPF record, and if it is, allows the email to be delivered as usual.

However, if the IP address or domain of the sending mail server is not listed in the sender domain's SPF record, it will either bounce the email back to the sender with an error or put it in the recipient's SPAM folder.

After analyzing what was causing email delivery errors, [admins noted](#) that Microsoft removed the '`include:spf.protection.outlook.com`' record from hotmail.com's SPF record.

To illustrate the issue, the previous SPF record for hotmail.com was:

```
v=spf1 ip4:157.55.9.128/25 include:spf.protection.outlook.com include:spf-a.outlook.com include:spf-b.outlook.com include:spf-a.hotmail.com include:_spf-ssg-b.microsoft.com include:_spf-ssg-c.microsoft.com ~all
```

Hotmail's [current SPF record](#) with spf.protection.outlook.com removed is now:

```
v=spf1 ip4:157.55.9.128/25 include:spf-a.outlook.com include:spf-b.outlook.com include:spf-a.hotmail.com include:_spf-ssg-b.microsoft.com include:_spf-ssg-c.microsoft.com -all
```

The [spf.protection.outlook.com SPF record](#) contains a large list of hosts allowed to send an email for the hotmail.com domain, and with that record missing, any email from those senders will fail SPF checks.

BleepingComputer tested sending an email from an Outlook.com Hotmail account and replicated the problem, with our email going to Gmail's SPAM folder instead due to its SPF record failing.

```
Authentication-Results: mx.google.com;  
    dkim=pass header.i=@hotmail.com header.s=selector1 header.b=Aoix6uEm;  
    arc=pass (i=1);  
    spf=fail (google.com: domain of ###@hotmail.com does not designate 2a01:111:f400:fe5b::808 as permitted sender) smtp.mailfrom=###@hotmail.com;  
    dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=hotmail.com
```

This is because the allowed IPv6 address (2a01:111:f400) associated with Outlook.com that was used to send my email is designated in the spf.protection.outlook.com record and, with its removal, is no longer accepted as valid.

Other hosts that will now fail SPF checks due to the removal of spf.protection.outlook.com are:

```
40.92.0.0/15  
40.107.0.0/16  
52.100.0.0/14  
104.47.0.0/17  
2a01:111:f400::/48  
2a01:111:f403::/49  
2a01:111:f403:8000::/50  
2a01:111:f403:c000::/51  
2a01:111:f403:f000::/52
```

Unfortunately, there is nothing that Hotmail users can do to fix this problem on their own, and they will have to wait for Microsoft to fix the DNS entry.

Update 8/18/23: Microsoft has told BleepingComputer that they have fixed the issue and Hotmail should no longer fail SPF checks.

Checking some of the SPF include statements for Hotmail.com, BleepingComputer has seen that they added some of the missing IP ranges to other includes, now allowing them all to properly pass SPF.

[DNS](#)[HOTMAIL](#)[PHISHING](#)[SENDER POLICY FRAMEWORK](#)[SPAM](#)[SPF](#)

LAWRENCE ABRAMS

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

[< PREVIOUS ARTICLE](#)[NEXT ARTICLE >](#)

Comments



buddy215 - 19 hours ago



It is back to normal for me. I just sent a hotmail email to a Yahoo one and it was received in one of my Yahoo acccounts....opened normally.