Outgoing emails marked as SPAM and Phishing emails by O365 servers

Discussion Options ...

ALV_Work OCCASIONAL CONTRIBUTOR

Apr 10 2019 08:51 AM

✔ Outgoing emails marked as SPAM and Phishing emails by O365 servers

Hi,

Since yesterday, all outgoing emails from our organization using Office365 (fully cloud) are being flagged as either spam or phishing email by Microsoft Outbound email servers. Due to this our Office365 user accounts are getting blocked every hour. We tried contacting Office365 support but they said they cannot help on outbound email spam settings as they do not have any control over the configurations. I spend more than an hour on the phone with the support person and at the end was asked [illegible] of them are getting flagged as either spam or phishing email, so sending random samples will not help. No spam or phishing filter settings have been changed since months now so I can only think on some backend updates done by O365 team for tightening the spam filters.

I am not sure whom to contact or escalate this case now so I am posting it in this group to everyone expecting someone who might have experienced the same might help. Any help to resolve this issue will be much appreciated as our users are unable to send emails.

Thanks.

View best response

Labels: Exchange | Exchange Online | Office 365

41.8K Views · 2 Likes · 32 Replies · Reply

32 Replies

All Discussions < >

Robin Nishad replied to **ALV_Work**

Apr 10 2019 10:42 AM

@ALV_Work

The issue seems quite strange. How did you know that MS Outbound servers are marking your emails as Spam. Secondly I hope your domain is still able to send emails to other domains, if yes... could you share a message header.. so that I can analyze it.

1 Like · Reply

ALV_Work replied to **Robin Nishad**

Apr 10 2019 11:13 AM

Hi@Robin Nishad ,

We have edited the default Outgoing Spam rule to copy messages flagged as spam to one of our internal email addresses. I have pasted the header from one such email (apparently we receive almost every outgoing email now) as requested. As you will notice that the Spam Confidence Level is set to 5 by Microsoft and the Phishing Level to 8 for this outgoing email from Office365. We do have even have 2FA enabled for most users and never had any issue till yesterday.

Received: from AM6PR0602MB3589.eurprd06.prod.outlook.com
(2603:10a6:208:aa::49) by AM0PR0602MB3585.eurprd06.prod.outlook.com with
HTTPS via AM0PR06CA0072.EURPRD06.PROD.OUTLOOK.COM; Wed, 10 Apr 2019
17:13:40
+0000
Received: from VI1PR0601CA0005.eurprd06.prod.outlook.com
(2603:10a6:800:1e::15) by AM6PR0602MB3589.eurprd06.prod.outlook.com
(2603:10a6:209:e::26) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.1771.19; Wed,
10 Apr
2019 17:13:39 +0000
Received: from VE1EUR01FT025.eop-EUR01.prod.protection.outlook.com
(2a01:111:f400:7e01::209) by VI1PR0601CA0005.outlook.office365.com
(2603:10a6:800:1e::15) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1792.14 via
Frontend
Transport; Wed, 10 Apr 2019 17:13:39 +0000
Received: from EUR01-HE1-obe.outbound.protection.outlook.com
(52.101.129.90)
by VE1EUR01FT025.mail.protection.outlook.com (10.152.2.232) with Microsoft
SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id
15.20.1771.16 via Frontend Transport; Wed, 10 Apr 2019 17:13:38 +0000
Received: from DB5EUR01FT040.eop-EUR01.prod.protection.outlook.com
(10.152.4.56) by DB5EUR01TH003.eop-EUR01.prod.protection.outlook.com
(10.152.4.138) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1750.16; Wed, 10
Apr
2019 17:10:53 +0000
Received: from EUR02-AM5-obe.outbound.protection.outlook.com
(52.101.131.59)
by DB5EUR01FT040.mail.protection.outlook.com (10.152.5.25) with Microsoft
SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id
15.20.1771.16 via Frontend Transport; Wed, 10 Apr 2019 17:10:53 +0000
Authentication-Results: spf=none (sender IP is)
smtp.mailfrom=anna.mandia@gmsuae.com;
Received: from AM0PR0602MB3554.eurprd06.prod.outlook.com (52.133.46.17)
by
AM0PR0602MB3523.eurprd06.prod.outlook.com (52.133.49.30) with Microsoft
SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
id
15.20.1792.14; Wed, 10 Apr 2019 17:10:45 +0000
Received: from AM0PR0602MB3554.eurprd06.prod.outlook.com
([fe80::9162:6e5e:65c1:9944]) by AM0PR0602MB3554.eurprd06.prod.outlook.com
([fe80::9162:6e5e:65c1:9944%6]) with mapi id 15.20.1771.014; Wed, 10 Apr 2019
17:10:44 +0000
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Anna Mandia <anna.mandia@gmsuae.com>
To: Calum Berkley <calumberkley@aol.com>, "reservations@milansuites.com.sa"
<reservations@milansuites.com.sa>, "ayman@milansuites.com.sa"
<ayman@milansuites.com.sa>, IBIS Abu Dhabi Gate FO3 <H6949-
FO3@accor.com>,
NOVOTEL Abu Dhabi Gate RE1 <H6948-RE1@accor.com>
CC: Paula Cercel <paula.cercel@gmsuae.com>, William Escondo
<william.escondo@gmsuae.com>, Amit Dagar <amit.dagar@gmsuae.com>
Subject: FW: Calum Berkley/Sharqi/12 Apr [Email Ref. #1457448]
Thread-Topic: Calum Berkley/Sharqi/12 Apr [Email Ref. #1457448]
Thread-Index: AQHU7g3sNf9KY9rzwEKdxrlIBbZyQaYySW2+gAAUiICAAtK0IA==
Date: Wed, 10 Apr 2019 17:10:44 +0000
Message-ID:
<AM0PR0602MB35543E59377335E66B1F11119D2E0@AM0PR0602MB3554.eurp
rd06.prod.outlook.com>
References:
<AM0PR0602MB35549FA31C962DC1097B472A9D2C0@AM0PR0602MB3554.eur
prd06.prod.outlook.com>
<AM0PR0602MB3554B2DF88EFB2AD15FCC0699D2C0@AM0PR0602MB3554.eur
prd06.prod.outlook.com>
<46AED3F05A1011E9B957005056BF25F3@focalscope.com>
In-Reply-To: <46AED3F05A1011E9B957005056BF25F3@focalscope.com>
Accept-Language: en-GB, en-US
Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-Exchange-Organization-SCL: 5
X-MS-TNEF-Correlator:
<AM0PR0602MB35543E59377335E66B1F11119D2E0@AM0PR0602MB3554.eurp
rd06.prod.outlook.com>
MIME-Version: 1.0
X-MS-Exchange-Organization-MessageDirectionality: Originating
X-MS-Exchange-Organization-AuthSource:
AM0PR0602MB3554.eurprd06.prod.outlook.com
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [217.164.74.77]
X-MS-Exchange-Organization-Network-Message-Id: 1516fec6-bb59-4dad-acf3-
08d6bdd77816
X-MS-PublicTrafficType: Email
Return-Path: anna.mandia@gmsuae.com
X-MS-Exchange-Organization-ExpirationStartTime: 10 Apr 2019 17:10:45.0518
(UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 2:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
X-MS-Office365-Filtering-Correlation-Id: 1516fec6-bb59-4dad-acf3-
08d6bdd77816
X-Microsoft-Antispam: BCL:0;PCL:0;RULEID:(2390118)(7020095)(4652040)
(8989299)(4534185)(4627221)(201703031133081)(201702281549075)(8990200)
(5600139)(711020)(4605104)(2017052603328)(49563074)
(7193020);SRVR:AM0PR0602MB3523;BCL:0;PCL:8;RULEID:(3031054)(100001)
(3032054)(3034054);SRVR:DB5EUR01TH003;
X-MS-TrafficTypeDiagnostic:
AM0PR0602MB3523:|AM0PR0602MB3523:|DB5EUR01TH003:|DB5EUR01TH003:|D
B5EUR01TH003:|DB5EUR01TH003:|DB5EUR01TH003:|DB5EUR01TH003:|DB5EUR0
1TH003:|DB5EUR01TH003:|DB5EUR01TH003:|DB5EUR01TH003:|DB5EUR01TH003:
|DB5EUR01TH003:|AM6PR0602MB3589:
X-MS-Exchange-PUrlCount: 3
X-Microsoft-Antispam-PRVS:
<AM0PR0602MB352364002DE092CC23D543D69D2E0@AM0PR0602MB3523.eur
prd06.prod.outlook.com>
X-Forefront-PRVS: 00032065B2
X-Forefront-Antispam-Report: SFV:SPM;SFS:(10009020)(136003)(39850400004)
(396003)(346002)(366004)(376002)(199004)(189003)(9686003)(3846002)(236005)
(52536014)(76176011)(4326008)(606006)(66066001)(25786009)(107886003)
(102836004)(53546011)(6506007)(26005)(186003)(11346002)(476003)
(71190400001)(66574012)(71200400001)(6116002)(790700001)(68736007)
(486006)(44832011)(33656002)(5660300002)(5024004)(446003)(14444005)
(97736004)(256004)(81156014)(81166006)(2201001)(54906003)(8936002)
(8676002)(508600001)(14454004)(110136005)(7696005)(53946003)(2906002)
(6306002)(2473003)(413944005)(99286004)(99936001)(316002)(229853002)
(74316002)(7736002)(2501003)(105586002)(6436002)(733005)(106356001)
(53936002)(55016002)(86362001)(54556002)(54896002)
(59010400001);DIR:OUT;SFP:1501;SCL:5;SRVR:AM0PR0602MB3523;H:AM0PR0602
MB3554.eurprd06.prod.outlook.com;FPR:;SPF:None;LANG:en;PTR:InfoNoRecords;
A:1;MX:1;
Received-SPF: None (protection.outlook.com: gmsuae.com does not designate
permitted sender hosts)
X-MS-Exchange-Organization-ExpirationInterval: 0:04:00:00.7865921
X-MS-Exchange-Organization-ExpirationIntervalReason: SpamEngine
X-MS-Exchange-AtpMessageProperties: sap=1;slp=1;
X-MS-Exchange-Transport-CrossTenantHeadersStamped: AM0PR0602MB3523
X-MS-Exchange-Transport-CrossTenantHeadersStripped: DB5EUR01FT040.eop-
EUR01.prod.protection.outlook.com
X-MS-Exchange-Organization-ACSExecutionContext: 04/10/2019
17:10:53;04/10/2019
17:13:38;{"SubmissionInfo":
{"SubmissionToken":"PFRva2VuIFRva2VuVHlwZT0iU3VibWlzc2lvblRva2VuIiBJZD0i
YjAyN2FkZWYtYjM1Yi1lOTExLWIwNzYtOWNkYzcxNTBlYjYyliBSb2xlPSJTdWJtaXR0
ZXIiIEVuZHBvaW50PSJodHRwczovL0hFMVNFVTA0VFAxMDUuZW9wLXNldTA0Ln
Byb2QucHJvdGVjdGlvbi5vdXRsb29rLmNvbS9zb25hcmFwaS8iIFNpZ25hdHVyZT0i
Rmg4aFlxVGszUkhDTDQ4S0NpK1haNEFWNlRBPSIgLz4","Identity":"9960c8bc-
7008-4852-a218-286be1ec6672"}};SC;S;0;04/10/2019
17:13:24;0|0|0|1|;
X-EOPAttributedMessage: 0
X-OriginatorOrg: gmsuae.com
X-MS-Exchange-Organization-SafeAttachmentProcessing:
X-MS-Exchange-Transport-EndToEndLatency: 00:02:55.2749479
X-MS-Exchange-Processed-By-BccFoldering: 15.20.1771.000
X-Microsoft-Antispam-Mailbox-Delivery:
ucf:0;jmr:0;ex:0;auth:0;dest:I;ENG:(20160513016)(750119)(520011016)(706158)
(944506303)(944610083);
X-Microsoft-Antispam-Message-Info:
DAPEWkLz3LKrnttMLdcI98FZqSXR7MZz4OAxsAZSkiO6Gu6jwVcQ8UY2dnhll4Er0h
SFzRtjFw1ahUoSQuNcF8JkUWZwJKBsg22Xejcz94WydHdk/2gZ33UC9IjWff1BjQEk
PJAxGAHyXXRwia3hCxqrFuM4MkRIX3wyAI+K67mNK5XXrlbmJta1l4mm2lRumAg
mngf4loOkKGF7eNyYO9VBQEImTYKVEimogNG/Gb1ZyvX+/Kxix7uGzdtR/9HQvQ
4cvulkEjoVIivTdX8XgPt0TH6nwFdG/kzjpCD4ufYIAb3HxGjsgrIgX7pGgKRgzg6xVO
dyFiihOo9Rr1+rxrU2/FdhsIbuKHPJM66JC02YId6Fot5bPkNgOSDDYBicG0HxUwsb
DMHbuE81ik85yTQrDCAx0lzwH4X6pWWIKzrCpVkclW79BujtKE1oPIb5WoPVj7n+
WiNIWDC59kEGqYYjX3BArXj3ohDEkRI2NMmfZMt2Sy6h0i6fPpcL/YngqxwQ2+pfx
DnWFJOCt4wNregwhu4gev2eR7CtduQohvInuqvP/rO62VOcX96b5HV5kmnTFZlQ
wr2OnnHNEKI85GXpIn9qvwxwxlS6g8TFI0EWpN4XRc0F0E8LA+k53Qmj/Zq64uvKj
55GIRE9AF4YmodBgxemEV6NdlF8t3xaM2FVEVC3pXGFthJ10VjUWzi2k5oeJSFYVv
mHHleLS61liPLiwic14OtMTvh8TgKTlnvvcOuhxFY6SlQLcrIMEgjsF1KaqPtTbkyrdu+
yY+raGdWajsnFM6lM7GETgaX/f90=

1 Like · Reply

Akshay_Mane replied to **ALV_Work**

Apr 10 2019 11:49 AM - edited Apr 10 2019 11:50 AM

@ALV_Work
This is the typical case of HRDP, when your outbound emails are detected as spam and EOP tries to deliver it to recipient with already blacklisted ip.

social.technet.microsoft. com/wiki/contents/articles/36402.exchange-online-troubleshooting-high-risk-delivery-pool.aspx

Looking at the headers, it seems that EOP IP 52.101.129.90 is on blacklist
Try to delist the IP on sender.office. com

Sometimes your tenant gets assigned a blacklisted IP in random. You can contact O365CloudExperts Support if you need more help.

Regards,
Akshay M

1 Like · Reply

Robin Nishad replied to **ALV_Work**

Apr 10 2019 12:05 PM

@ALV_Work

I noticed in the Message Header -

Received-SPF	None (protection.outlook.com: gmsuae.com does not designate permitted sender hosts)

So would suggest to check if the sender domain is added in the allowed domain settings in Security and Compliance center.

1. Sign in to O365 Admin Portal
2. Navigate to Security & Compliance center > Threat management > Policy.
3. Find Anti-spam, open it. Expend Allow lists. Add the sender's domain to the Allow domain setting.

1 Like · Reply

ALV_Work replied to **Robin Nishad**

Apr 10 2019 12:40 PM

Hi@Robin Nishad ,

Thanks for the suggestion. We already have the domain added in the Allow list of Anti-Spam policy.

Could it be that the domain is showing as SPF not designated because it is still an internal email within Office365 servers ?

1 Like · Reply

Robin Nishad replied to **ALV_Work**

Apr 10 2019 12:52 PM

@ALV_Work

if the Domain is added in the Allow list, then I would suggest to submit the message to MS and let them know that it is not Spam. I know & understand that you are already working with MS on this however I would like you to refer to the steps given in the below article....

https://docs.microsoft.com/en-us/office365/securitycompliance/submit-spam-non-spam-and-phishing-scam...

(Submit messages that were tagged as junk but should have been allowed through)

Secondly the proof that MS Servers are marking your email as Spam is that in the header - Anti Spam Report - It has SFV-SPM that means the email is marked as Spam because of the EOP Spam filters.

Reference Article - https://docs.microsoft.com/en-us/office365/SecurityCompliance/prevent-email-from-being-marked-as-spa...

Moreover do check if the emails that you are sending has any HTML Signatures or they are simple text.

1 Like · Reply

Philippe_RAYNAUD replied to **ALV_Work**

Apr 11 2019 11:35 AM - edited Apr 11 2019 11:55 AM

@ALV_Work We got exactly the same problem yesterday, I opened a ticket but Microsoft seems to have no clue about what happened.

We worked on it a while and this is what we could figure out about our case :

- It started around 7am CET and ended around 8pm CET
- It has nothing to do with SPF or whatever
- EOP was giving a SFV:SPM SCL:5 to outbound emails ONLY IF they were replies or forwards to external email addresses, so they were using the High Risk Delivery Pool and we were getting a BCC in our IT mailbox as our Outbound spam Policy specifies it. I can see in your header that it was the same for you : DIR:OUT;SFP:1501;SCL:5
- When an external person was answering one on these emails they were coming back with SFV:SPM and CAT:PHSH, so we got PLENTY of emails yesterday ending up in junk folder
- Every Outbound Spam BCC in our IT mailbox arrived twice, the second time with a huge delay (6+ hours), and message stayed in "Getting Status" for very long time in traces, maybe because they were going through the High Risk Pool.

We didn't make any changes in our SPF or policies, it just randomly happened and ended.

I'm still waiting for an explanation from Microsoft.

2 Likes · Reply

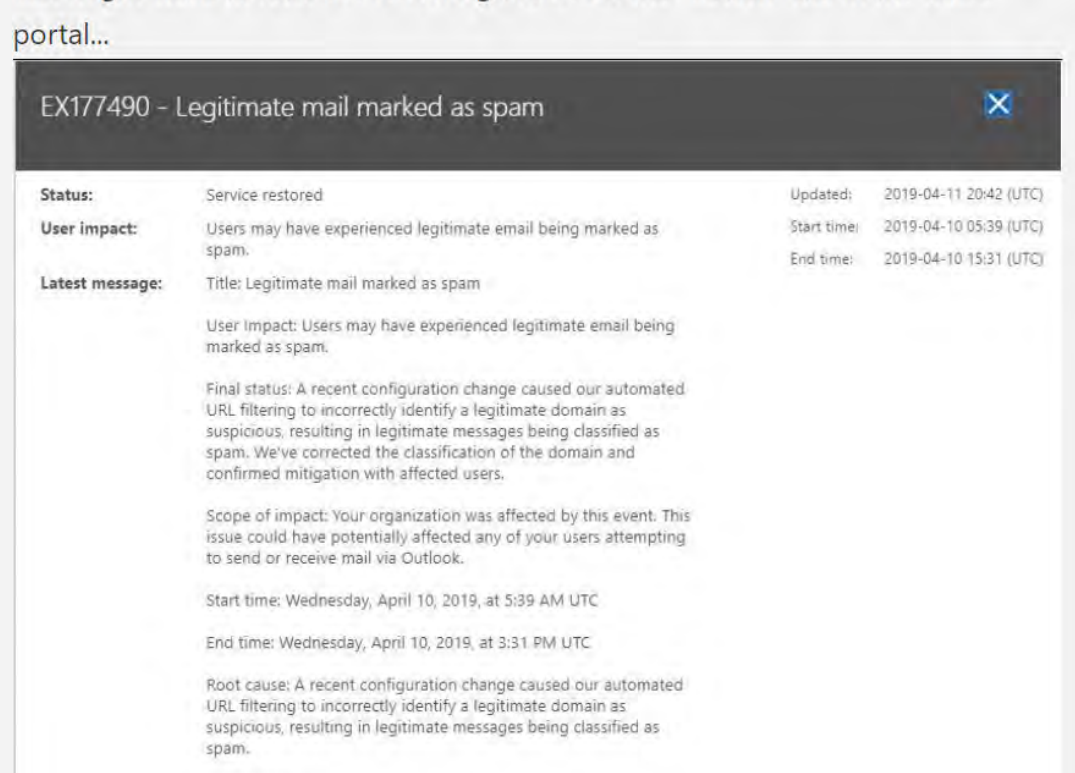
best response confirmed by ALV_Work

Rafmoerkens replied to **Philippe_RAYNAUD**

Apr 12 2019 12:05 AM

✔ @Philippe_RAYNAUD

You might want to read the following article on the "health" tab in the office portal...



3 Likes · Reply

Philippe_RAYNAUD replied to **Rafmoerkens**

Apr 12 2019 12:30 AM - edited Apr 12 2019 12:32 AM

@Rafmoerkens Thanks for this, It doesn't appear in my portal, I only have the "EX176985 - Can't see message traces" ...

1 Like · Reply

Rafmoerkens replied to **Philippe_RAYNAUD**

Apr 12 2019 12:33 AM

@Philippe_RAYNAUD: you might have been "out of scope"? ;)

@ALV_Work: please see above as you were the one that had the issue :)

1 Like · Reply

ALV_Work replied to **Rafmoerkens**

Apr 12 2019 01:02 AM - edited Apr 12 2019 01:02 AM

Hi@Rafmoerkens @Philippe_RAYNAUD ,

Negative. Had a call from O365 support guy(not direct MS staff) and he has confirmed that my domain is having a service incident but I still donot see anything on my office portal. But looks like the issue is not happening now.

1 Like · Reply

ALV_Work replied to **Philippe_RAYNAUD**

Apr 12 2019 01:08 AM

Hi @@Philippe_RAYNAUD ,

All the scenarios mentioned by you is the same for me too. Got a lot of emails tagged as PHISH by AntiSpam policy and all went into quarantine due to our Antispam settings. Had to release them manually to the users. Also we got a lot of duplicate emails send as BCC to our IT email address since outgoing emails where getting tagged as SPAM. But now the issue seems to be have stopped. Looks like MS Team has reverted the changes.

1 Like · Reply

Philippe_RAYNAUD replied to **Rafmoerkens**

Apr 12 2019 01:30 AM

@Rafmoerkens Their article is weird though, I don't understand what this has to do with "URL filtering"! Happened with every single message.

1 Like · Reply

ALV_Work replied to **Philippe_RAYNAUD**

Apr 12 2019 10:50 AM

Hi @Philippe_RAYNAUD @Rafmoerkens

May be something to do with links in signature of outgoing emails.

1 Like · Reply

Philippe_RAYNAUD replied to **ALV_Work**

Apr 12 2019 03:29 PM

@ALV_Work Nope we tried with blank messages was the same, I think we will never know what really happened :)

1 Like · Reply

Sujesh1415 replied to **ALV_Work**

Sep 16 2019 05:32 AM

We are facing same issues from past week. Did create a ticket with MS and is still being worked on.

We didn't make any recent changes to any of our policies and wondering what is the reason behind it. Its been a week that we are exchanging mail headers and extended message traces and didn't reach to isolate the issue yet.

0 Likes · Reply

ALV_Work replied to **Sujesh1415**

Sep 16 2019 05:58 AM

Hi @Sujesh1415 ,

Only Microsoft Team can resolve this issue. It mostly due to an issue at their servers which tags outgoing emails as spam. This affects not everyone i guess just random tenants.

0 Likes · Reply

Jordan160 replied to **ALV_Work**

Jan 23 2020 09:17 AM - edited Jan 23 2020 09:26 AM

@ALV_Work

I'm having a similar issue with a client who has Office 365 for email.

Their domain name was categorized as CAT:HPHISH due to their website being hacked. Once cleaned up they started having emails being quarantined. They put their domain name in their signature. So any customers they emailed with Office 365 wouldn't get the email, it would be quarantined. When a customer who wasn't on Office 365 got the email and replied, the client wouldn't get the email.

We've reached out to Microsoft Support, however, they're unable to understand what needs to happen. And there is no system in-place to change/remove domain names from this categorization. Even though they have https://sender.office.com for de-listing IP addresses, there is no way to submit domain names.

Other vendors like PaloAlto, FortiNET and Sohpos provide the means to submit evidence for delisting domain names categorized as Phishing or Spam.

EDIT: The only method I see to report the domain name as a false positive or have the category changed or removed is through the Office 365 Protection Portal under the "Quarauntine Queue", by clicking "Submit Message" with no information on where it's going or if I will get notified if any action was taken.

The other method is in a Microsoft article https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/submit-spam-non-spam-and... which states "Use the same procedure as described in the "Use email to submit junk (spam) or phishing scam messages to Microsoft ," but send the message to not_junk@office365.microsoft.com."

Tags: 3

0 Likes · Reply

EmailIssues replied to **Jordan160**

Jan 23 2020 02:22 PM

@Jordan160

We are having the exact same problem. Tomorrow will be our 3rd day of being mostly down and working with 0365 who can't figure out the problem or even understand that it is bigger than analyzing a couple email headers.

Is there a way to get in contact with higher tier support that has more to say than " tell your recipients to whitelist you."?

0 Likes · Reply

< 1 2 >

Outgoing emails marked as SPAM and Phishing emails by O365 servers

Discussion Options ...

ALV_Work OCCASIONAL CONTRIBUTOR

Apr 10 2019 08:51 AM

✔ Outgoing emails marked as SPAM and Phishing emails by O365 servers

Hi,

Since yesterday, all outgoing emails from our organization using Office365 (fully cloud) are being flagged as either spam or phishing email by Microsoft Outbound email servers. Due to this our Office365 user accounts are getting blocked every hour. We tried contacting Office365 support but they said they cannot help on outbound email spam settings as they do not have any control over the configurations. I spend more than an hour on the phone with the support person and at the end was asked to send 5 sample emails to not_junk@office365microsoft.com and wait for 48 hours. I told O365 support that each user who is blocked sends around 100 emails of which all [illegible] tightening the spam filters.

I am not sure whom to contact or escalate this case now so I am posting it in this group to everyone expecting someone who might have experienced the same might help. Any help to resolve this issue will be much appreciated as our users are unable to send emails.

Thanks.

View best response

Labels: Exchange Exchange Online Office 365

41.8K Views 2 Likes 32 Replies Reply

32 Replies

All Discussions < >

Jordan160 replied to **EmailIssues**

Jan 23 2020 03:06 PM

@EmailIssues

Yes, you need to keep calling them. They have access to remove the domain name from their internal list. We just got this completed by their support.

0 Likes Reply

EmailIssues replied to **Jordan160**

Jan 27 2020 06:52 AM

@Jordan160

Unfortunately we have not been so lucky. Dozens of calls and we are still down. No one at Microsoft seems to care.

Do you happen to have a MS description of what they did to resolve your issue or a ticket # I can share with support?

I could maybe understand this run around if this was a small company, but they have nearly 100 users. I can not believe the lack of support we are getting.

0 Likes Reply

Jordan160 replied to **EmailIssues**

Jan 28 2020 08:50 AM

@EmailIssues

I'm sorry to hear that. You have to be persistent and point them to this post and ask for an escalation.

Unfortunately, I am unable to provide the ticket number due to the privacy of the client. However, this is what was communicated by the person who got ahold of someone at Microsoft after 8 hours of total time with their support staff. They also had to make sure they had the appropriate SPF/DKIM/DMARC records in-place before they would even consider looking further.

> Basically, there are third-party lists that scan sites looking for phishing stuff, they had found domain name to be a part of that.
>
> They are working on clearing off the domain from those lists, and while that's being done Microsoft is clearing the domain from the watchlist at the moment.
>
> It should take a couple of hours for it all to propagate and take effect, and he will be calling me when it's all done.

0 Likes Reply

EmailIssues replied to **Jordan160**

Jan 28 2020 09:11 AM

@Jordan160

Thank Jordan. We have several tickets open two of which have been escalated. We provided the link to this thread with no luck. We have ~30 hours into this client and MS support now.

Seems like your luck is better than ours lol. I will keep my fingers crossed that the description provided helps but it's pretty much what we already told them.

0 Likes Reply

Jordan160 replied to **EmailIssues**

Jan 28 2020 09:16 AM

@EmailIssues

That really sucks, trying to get past the first line of support is the hardest.

As long as you have the headers stating the category, it should pretty straight forward to resolve. It's just trying to get someone from support who actually understands what needs to happen or have them escalate it to someone that knows.

I'm going to post this resolution to Reddit just-in-case MS decides to lock this thread or delete it.

It's a shame that support can't understand their own technology stack to identify and issue and provide some sort of resolution. This type of process resolution has been in place with other vendors like PaloAlto, Fortinet and Sophos for years.

1 Like Reply

EmailIssues replied to **Jordan160**

Jan 28 2020 01:16 PM

@Jordan160

Update: They finally did it!

Here is the text from MS if anyone needs it to point support in the right direction.

Hi **,**

Hope all is well. My name is * from Office 365 Next Team,**
We received an escalation request with regards to your issue on spam emails. After further investigation www[.]********[.]com was listed as a phish URL, it appears the site may have at one time been compromised but is no longer. We have properly delisted it. Can you please check if your emails are still ending into spam/junk folder?**

Thank you,

****
Office 365 Next Team

0 Likes Reply

Jordan160 replied to **EmailIssues**

Jan 28 2020 03:05 PM

That's awesome!

0 Likes Reply

Asif Rehmani replied to **EmailIssues**

Jan 29 2020 03:36 PM

Wow. this seems scary. you should not have had to go through all this before finally getting this fixed. Glad it all got figured out though.

0 Likes Reply

apsimm replied to **EmailIssues**

Feb 05 2020 04:20 AM

@EmailIssues

I'm having this issue with three of my personal MSFT email accounts, not through O365. I can receive emails but all my sent emails are being returned by the protection.outlook.com server. It won't even let me send an email to myself. Weird thing is that i can send emails from same accounts on my phone.

Any thoughts on who I can contact or do I just assume this is a bigger problem and hope it works itself out. Thank you.

0 Likes Reply

MaxWinterstein replied to **apsimm**

Feb 11 2021 02:36 AM

I've been through this now **two** times.

Every email containing my domain was marked as high confidence spam on every O365 tenant I know. On my own, as well as on customers. Even at the bare minimum, a plain text email containing just "myDomain.org" was marked as spam.

I knew about some spam incident involving our domain as an email sender from non O365 servers that fits around the starting time of the issue at the first occurence. For the second incident there is no realted event known to me.

Both times I have been hours in the Hotline with supportes that were honestly friendly and trying their best but tried everything to not move my ticket to second level support. They stick to their checklist and did not really take care of my mentions. E.g. he tried thousand times 'https://www.myDomain.org' at mail rules and stuff, even i showed him dozent times 'myDomain.org' was sufficinent.

Both times it seemed to resolve itself after roughly 7 days, which lets me think their internal filters drop after one week. Support guy told me that they were working hard on my ticket and someone fixed it...
After the supporter saw the issue resolved itself the ticket was closed. Definetly not satisfiying.

There is some panel the support guy pointed me towards: https://protection.office.com/reportsubmission where you can submit URLs that should not be marked as spam. If this is any good? Idk.

Not sure if this has already been posted here, but another good link I found about this: https://www.reddit.com/r/Office365/comments/ev98sd/an_issue_with_a_microsoft_office_365_customers/

So i am sitting here, waiting for the next time this starts to happen...

0 Likes Reply

Jordan160 replied to **MaxWinterstein**

Feb 11 2021 11:53 AM

@MaxWinterstein I made that Reddit post. It's a shame Microsoft doesn't have a means to resolve the issue you're facing. When a organization get's so big, really difficult issues like this seem to slip through the cracks.

0 Likes Reply

SChicora replied to **ALV_Work**

May 26 2021 02:05 PM

Our organization is having this issue with incoming and outgoing mail. I have had our users remove the weblink from their signature line, after speaking with a Microsoft Tech, and mail is flowing out from us without being rejected now. Today, we have started to see that all mail, with any type of link in it, is going into our Junk Folders. Both internal and external.

0 Likes Reply

ExpertInstitute replied to **SChicora**

Dec 08 2021 11:58 AM - edited Dec 08 2021 12:16 PM

Our organization is also experiencing the same exact issues with legitimate / wanted emails that our clients are expecting. These emails are being quarantined / sent to spam, or even rejected in some cases, specifically by Microsoft 365 / Outlook receiving servers.

We've been thoroughly testing and it appears to be specific to our domain and not related to our email sending platforms or IPs. This issue has been persisting across our entire organization for the last 6 weeks. Our DKIM / SPF records are all setup correctly. We're using Dmarcian, HetrixTools to monitor / confirm our DNS settings. And we've also had two email deliverability consultants check our domain settings and confirm that they believe this is an internal false flag on Microsoft's side.

After speaking with numerous Microsoft support staff, we've finally made contact with an escalation team and have provided them with email samples of quarantined / rejected emails, which are all wanted by our clients. This issue is severely impacting our business, as our clients are unable to receive emails / work product for which they have already paid.

I'm hoping that someone from Microsoft's Team can kindly escalate this issue and advise us on next steps to delist our domain from their internal blacklists.

0 Likes Reply