https://forum.directadmin.com/threads/microsoft-outlook-blocking-your-mail-server.70445/

Microsoft/Outlook blocking your mail server?
Thread starter Kal Start date Apr 4, 2024

Kal Verified User
Joined Nov 18, 2019
Messages 139
Location Australia

Apr 4, 2024 #1

Every few months Microsoft blocks our server. We then have to go through the tiresome process of making a delisting request, waiting for the email from Outlook support saying, 'Nothing was detected to prevent your mail from reaching Outlook.com customers', responding to that email to say that our server is still blocked, then waiting for them to delist the server. If I ask them why they blocked us (which I've given up doing now), I get the same response every time: 'we do not have the liberty to discuss the nature of the block'. Needless to say, I'm over it.

Anyone else having a similarly painful experience? I have to assume it's a fairly common experience, because between our delisting requests in November and March, our Outlook.com case numbers incremented by 9,393,678. That's over 9 million support requests in 4 months. I'm not saying they were all delisting requests, but people don't fill out a deliverability support form for fun.

I found this discussion from 2020, which talks about mail going to spam for recipients with Microsoft (Outlook, Hotmail and MSN) email accounts. In that thread, the focus was on working with the very nice and helpful people at Microsoft to get delisted—celebration! That's fine if it happens once. When it happens over and over and over again, one grows a little more cranky and cynical.

I also found this discussion on the Outlook forum. One user noticed that Microsoft is mangling the signed headers, causing DKIM to fail. Like others, I too have noticed that some Microsoft DMARC reports show DKIM failure, whereas reports from other mail providers pass DKIM every time.

Admittedly, I'm no expert, so I'm hoping someone else can shed more light on this. Are we wrong to conclude that Microsoft is just incompetent when it comes to mail authentication and is repeatedly blacklisting correctly configured and well behaved mail servers for no good reason at all?

johannes Verified User
Joined Feb 18, 2007
Messages 990

Apr 4, 2024 #2
I`d suggest to register your IP within the MS SNDS
https://sendersupport.olc.protection.outlook.com/snds/

Reactions: Richard G Kal Verified User
Joined Nov 18, 2019
Messages 139
Location Australia
Apr 4, 2024 #3

@johannes, I am enrolled in both SNDS (Smart Network Data Service) and JMRP (Junk Mail Reporting Program) and neither have been helpful at all. My IP always has 'normal status', there's never any data for my IP on any date I select, and I haven't received a single junk mail report.

Reactions: gozen and Richard G
Kal Verified User
Joined Nov 18, 2019
Messages 139
Location Australia
Apr 4, 2024 #4

This happens so frequently, I have a written process for it now. In case it helps anyone else, my delisting process is this:

Go to the Office 365 Anti-Spam IP Delist Portal at https://sender.office.com and submit the form. (This rarely, if ever, works. If the delisting request is denied, don't bother clicking the link requesting an escalation. Go to step 2 and open an Outlook support ticket.)

Submit a delisting request at https://olcsupport.office.com. Sign in using [email address]. (If you sign in with your username the contact email field gets automatically populated with this and can't be changed!)

Check that the form has been submitted properly. At the top of the screen it should say 'Thank you - your request was submitted'. If the page just refreshes without this message, it failed silently and you need to work out what field is causing the problem. It seems to fail if you try and include multiple domains in the 'What domain are you sending from?' field, or if you enter too many characters in the 'Copy and paste any error messages' field (even though it truncates the text).

(Optional) Log in at https://sendersupport.olc.protection.outlook.com/snds/ and click on 'View IP Status' and 'View Data'. (This has never given me useful information in the past, but it may be worth a try.)

Wait for the email from Microsoft saying, 'Nothing was detected to prevent your mail from reaching Outlook.com customers' and reply, 'I can assure you, Outlook.com is blocking our mail server. You already have all the details in the support request. Again, the IP of our server is [IP address].'

Wait for the email from Microsoft saying, 'We have implemented mitigation for your IP…'.

You can waste a LOT of time (as in weeks) if you end up talking with the wrong Microsoft support people, so I've learnt from painful experience to just skip to step 2.

Reactions: Waqass, johannes and toml
Richard G Richard G Verified User
Joined Jul 6, 2008
Messages 14,026
Location   Maastricht

Apr 5, 2024   #5

A very good cause of this can be Microsofts dynamic spam filter. Which is used by hotmail/outlook users for example.
You won't get notices about that either from SNDS/JMPR and it's very disturbing.

We discovered some of the causes of this. We had some forums on the servers, which ofcourse send happy birthday messages to users and also thread notifications on threads they themselve subscribed to with e-mail notification.
Seems some people rather report these birthday messages and thread notifications as spam, than just unsubscribe from those notifications or ask the forum admin to remove their account.

Same happened with another customer, which has a webshop where people subscribed to the newsletter, did not sign off but just moved them in their hotmail to the spamfolder.
And ofcourse same was happening for autoreply's others were using and which were sometimes abused by spammers.

This kind of behaviour logically resulted in regular greylisting by Microsoft. And indeed it takes time to get the ip out of there again.
Average 3-5 days easily with having to do the forth and back mailing with Microsoft indeed, so yes can take weeks if it happens more often.

Being a member of SNDS and JMPR still is helpfull, as sometimes you can get notice, but also you can use the argument in your mail to MS, that you did not have any notification via SDNS/JMPR and your ip is not in any blacklist. MS will see membership of SNDS/JMPR as a pré as they also advise to be a member.

Hardly anything you can do about it, except for trying to figure out as to why this is happening again. And maybe you can find something by the examples I gave.
The forums stopped sending birthday messages and thread notifications now with other software have an unsubscribe link. Most of my customers do not use auto-reply's as advised.
So we haven't been on the list anymore for several years.

But it's no guarantee. It can be very hard to get and keep of that list. Even if you try hard.

Kal Verified User
Joined Nov 18, 2019
Messages 139
Location Australia

Apr 5, 2024 #6

Richard G said:
Seems some people rather report these birthday messages and thread notifications as spam, than just unsubscribe from those notifications or ask the forum admin to remove their account.

Yeah, not much we can do about some people! ?

Thanks for sharing your experience Richard. I do have one or two users who send out hundreds (not thousands) of emails, and there's always a chance some recipients are labelling it as spam, but I suspect it has more to do with Microsoft's incompetence. We are such a small shared server with nothing but good honest, people—we are not sending out spam or scam emails. It's so frustrating to have your whole server (single IP address) blocked by a big company with zero accountability to small businesses like us. This is just another example where the little guy suffers from the practices of big corporations. You can be sure that Microsoft will never block the whole Gmail network regardless of how much spam originates from it!

Richard G Richard G Verified User
Joined Jul 6, 2008
Messages 14,026
Location Maastricht

Apr 6, 2024   #7

It's the same here, we also have a small server with around 60 accounts on it and that's it.
And in the beginning it was even less, more like 40 when we were in your situation.
It also just takes time to build a certain repuration, even if it's a neutral reputation. We noticed that when starting a new vps which we temporarily used to move servers and devide accounts. And then this server came onto a Spamhaus list, got it of, 2 weeks later it was on again, got it off again and after that it got on the list and I didn't get it off again.
Reason: the main server domain we used was new and not known to send mail yet, we had to build a reputation first. Hard to do when mails get blocked. ;)
Big company's pay for some kind of whitelisting and then they don't block each other. It's always the small company's who are hit worst. On the other hand, it's mostly also that most spam is coming from small company's and vps providers.

toml Verified User
Joined Oct 3, 2003
Messages 1,261
Location   Scottsdale, AZ
Apr 6, 2024   #8

It does make me happy to see a ton of Microsoft's email servers flagged on bl.spamcop.net. I have had a bunch of email rejected because Microsoft wasn't cleaning up their own reputation.

Reactions: Kal, johannes and Richard G
Richard G Richard G Verified User
Joined Jul 6, 2008

Messages 14,026
Location Maastricht

Apr 6, 2024   #9

LoL... fun to see they are on Spamcop. :D
However, that will not take long, just as with Ziggo which sometimes comes on there, mostly it's for a few hours or max a couple of days.

I even reported several microsoft accounts to Spamcop this week. :)
Microsoft doesn't even obey the RFC's. When I have SPF and DKIM and DMARC, the only time I get notices from easydmarc about things maybe went wrong, is if it's forwarded to a Microsoft account, because MS rewrites the headers and then it looks like the original sender is MS. Which MS isn't. Only happening with MS, not with Gmail or any other system.

Kal Verified User
Joined Nov 18, 2019
Messages 139
Location Australia
Apr 6, 2024 #10

Richard G said:
… because MS rewrites the headers and then it looks like the original sender is MS. Which MS isn't. Only happening with MS, not with Gmail or any other system.

Yes, which makes our email fail DKIM, as I mentioned in the original post. It'll still pass DMARC if SPF passes, but if the email gets forwarded that will fail too. Then you get penalised for Microsoft's incompetence!

Richard G said:
On the other hand, it's mostly also that most spam is coming from small company's and vps providers.

Have you got some stats on that? I imagine a lot of spam comes from Gmail and Microsoft accounts, but I have no stats to back that up. When I was regularly reporting on Spamcop, I was seeing the same offenders over and over again. QuadraNet immediately comes to mind.

Richard G said:
Big company's pay for some kind of whitelisting and then they don't block each other. It's always the small company's who are hit worst.
Yep, that's how the world works. If you have enough money you can buy anything and pass the buck when things go wrong. The billionaires are screwing over the world but most people are too focused on migrants and dole-bludgers to notice!

Richard G Richard G Verified User
Joined Jul 6, 2008
Messages 14,026

Location Maastricht

Apr 7, 2024 #11

Kal said:
Have you got some stats on that?

www.mailmodo.com
23 Email Spam Statistics to Know in 2024
Find out the absurd amount of spam emails sent by people from certain countries, different types of email spam statistics like phishing emails, etc.
www.mailmodo.com
US is the biggest, but I also look on our servers and from Gmail and Microsoft we got the least spam.

So this can be different from what your experience is, but on our servers that is the case.
Some big company's with VPS selling have a hard time fighting spam. Quadra is one of them, but there are also who really provide spam. I just check how often I get spam from them via Spamcop, and at a certain point I'm fed up with them and then I block their complete ASN in Exim.
There is a German company who has serveral ASN's and had send loads of spam to us.

Reporting to Spamcop is still a good thing. And I will keep doing that and keep blocking abusers who keep coming back.

Reactions: Kal Kal
Verified User
Joined Nov 18, 2019
Messages 139
Location Australia

Apr 7, 2024 #12

Those stats don't really say whether Spam is coming from big or small networks, but they are still interesting. While email is hailed as the only truly open global communication standard, what does the fact that over 45% (84% during COVID lockdowns!) of emails are spam tell us? From a technical point of view, I think it supports the view that SPF, DKIM and DMARC little more than bandaids on a fundamentally broken system. From a philosophical point of view, it tells us that humans are kind of broken too—whenever we create something good, the greed of a few will spoil it for the many. :confused:

Agreed, Spamcop is a good thing. I go through phases of having the energy to report, and phases of 'I couldn't be bothered'.

Richard G Richard G Verified User
Joined Jul 6, 2008
Messages 14,026
Location Maastricht

Apr 7, 2024 #13

Kal said:
it tells us that humans are kind of broken too—whenever we create something good, the greed of a few will spoil it for the many. :confused:

Unfortunately that was always the case and most likely will never change. :(

Thoses phases are well known to me too. Sometimes I don't bother either, but since I'm not too busy, I'm just having fun reporting them. Also I use the Abuseipdb reporter. Have a script for it and it automatically reports abusing ip's.

johannes Verified User
Joined Feb 18, 2007
Messages 990

Apr 7, 2024   #14

Richard G said:
Also I use the Abuseipdb reporter. Have a script for it and it automatically reports abusing ip's.

Would you mind to elaborate and share it, please?

Richard G Richard G Verified User
Joined Jul 6, 2008
Messages 14,026
Location Maastricht

Apr 8, 2024   #15

Sure. AbuseIPDB you can look in Abuseipdb.com you can use an account then more ip's can be reported.
You can use AbuseIDB in CSF and also use the AbuseIPDB blocklist if you want.

The script is great and is from @eva2000 who created it. It has all kind of options, even customizable and reports.
You can find it here including complete documentation:
github.com
GitHub - centminmod/centminmod-abuseipdb-reporter: CSF Firewall and AbuseIPDB API integration with specific focus on data privacy and prevention of sensitive data leaked to public AbuseIPDB database report
CSF Firewall and AbuseIPDB API integration with specific focus on data privacy and prevention of sensitive data leaked to public AbuseIPDB database report - centminmod/centminmod-abuseipdb-reporter
github.com github.com

Reactions:
Kal, johannes and eva2000
johannes Verified User
Joined Feb 18, 2007

Messages 990

Apr 9, 2024 #16

Ah, good to know, thank you very much. I have already an account there, but was not aware of automating things.