MetaCompliance

Summer PowerUser Series Phish Allowlisting

Here's what you asked ...

Q: We use a URL Bypass Policy in Mimecast, we have to specify the domain as part of the configuration, is there anyway I can include all the domains which Metacompliance use, to save adding each one for each phish??

A: What we would recommend in terms of having to add specific URLs or domains, is using wildcards against the domain.

Q: What is the reason why some of the users do not receive the simulation? If it gets blocked by Mimecast?

A: If the emails are getting blocked by Mimecast, usually the main reason would be that the allow listing hasn't been set up correctly, meaning they could be marked as spam, which you should be able to see within the Mimecast logs which have stopped that from moving through and to Microsoft or your mailbox.
Please reach out to our support desk and an agent will pick up your request and have a quick call on it.

Q: Is there any way to keep the simulated URL list on the MS Advanced Delivery dynamically up to date?

A: If you've got the IPS and the dedicated DKIM domain in there, it should be up to date, unless there's an infrastructure change on our side which you would be made aware of in advance.

Q: So, generally, if I see that the IP in the Phish Audit is one from Microsoft Corporation, it means it was the false-positive?

A: Typically, it does. Using the steps that we went over on the call will completely confirm for you that it was a false positive.

Q: Why there are false positives for some of the users, but real results for others, in the same campaign? Does Microsoft check some emails, and doesn't check others? We've setup the Allowlisting as per MetaCompliance documentation.

A: With Microsoft and most security vendors, what they do is what's called sampling. If you send a phish to a bulk number of users, instead of them scanning all the emails, they would sample a number of the emails that's going through. They would then sandbox them and scan them for malicious content that way.
If you've set up the allowlisting as per our documentation, it may be the case that the emails are getting rewritten, so we'd mentioned on the session about the authentication results header.

Q: Can you remove the false positive from the data for a user so that the user is not flagged as a recurring victim?

A: Please contact our Support Desk to look into this with you, as we would recommend having correct allowlisting in place before going live with a phish.

Q: Is there a way to get results from Microsofts report phish button into MetaCompliance reports?

A: Not at this moment.

Q: For configuring Exchange Online to not interact with emails from a specific domain, does MetaCompliance have documentation on this?

A: All relevant allowlisting documentation can be found: https://support.metacompliance.com/hc/en-gb/sections/5961204975889-Allowlisting

Third Floor, Old City Factory,
100 Patrick Street, Londonderry BT48 7EL
t: +44 (0) 28 7153 9777 **e:** info@metacompliance.com
www.metacomplicance.com

MetaCompliance

MetaCompliance

Summer PowerUser Series Phish Allowlisting

Here's what you asked, Continued ...

Q: Just wondering why domains that have been setup & whitelisted across our services worked in one campaign without false positives then not in another. Whitelisting even using the same domains and links seems to be a moving target.

A: If the IP addresses and domain matches with what's in advanced delivery then there may be something else at play. Has there been any additional or any changes at all to that phish? If you've used the same domain and you've still got the IPS and domain within your whitelisting and you're seeing these issues. Has anything changed since the first campaign? Is there any changes within the phish? Have you used anything extra? Attachments or QR codes for example.

Q: What about "False Negatives"? We had a problem with a simulation recently, where some users clicked the links within one mail and advanced to the results page, but MC didn't register them as "clicked".

A: Please reach out to Support in this scenario, and we will investigate this with you. We'd be interested to look into that to see if there's any traffic that's stopping those requests being sent to us.

Q: I suspect we have a false positive situation for a user using a mobile device - would we investigate this the same way?

A: For mobile devices, still heavily rely on the reporting section, so if you do look at the IP address column and then do an IP look-up on that, it should bring you back the ISP.

Thank you to everyone who attended our webinar on 14/08/2024. We greatly appreciate your participation and engagement, and we hope you enjoyed the session.

We have more exciting content coming soon. In the meantime, please make sure to sign up for our upcoming events, which will be held until the end of August. You can register for these events ***HERE.***

Laura Wade - Head Of Customer Experience

Make it personal.

Don't Miss Our Upcoming Summer Power Sessions - Get Registered Here!

Third Floor, Old City Factory,
100 Patrick Street, Londonderry BT48 7EL
t: +44 (0) 28 7153 9777 **e:** info@metacompliance.com
www.metacomplicance.com

MetaCompliance