ABOUT
Mimecast Protections

Mimecast email security is always working to keep your company protected. Here we explain the activities and what you can expect.

Anti-Spoofing

What it is: Anti-Spoofing prevents an external actor from using your exact domain name to target your organization, which is a very common activity.

What to expect: When Anti-Spoofing is active, no email using the company's domain will be permitted to pass through Mimecast. This means that any third party tools (such as SalesForce or HubSpot) that have permission to use your email will not be permitted and must be whitelisted (i.e. allowed). Corvid Cyberdefense will conduct periodic reviews to ensure that any of your required tools that were added are unblocked. Change requests can also be requested through our support portal.

Attachment Management

What it is: Attachment Management is designed to detect file types and stop the delivery of known bad file types. These are file types that are typically not sent via email and usually are used to allow more advanced actions upon your machine. For example, an executable file (.exe) could allow a hacker to open up a back door.

What to expect: This policy is typically unnoticed as most companies do not use unusual file types. However, encrypted, archived, and/or compressed files can be selected to be blocked and this could lead to attachments being held for incorrect reasons. If a file is incorrectly held, a support request can be placed. This would lead to either one-off actions or edited policies to prevent future events.

Attachment Protection

What it is: Attachment Protection is designed to have all attachments checked, similar to a TSA airline security check, to ensure nothing malicious is hidden within the file.

What to expect: In most cases this is unnoticed for the user, but in some cases, if the file is large for example, you may receive an email moments before the attachment arrives. In these cases, a banner will be added to the email and then after a few minutes the attachment will be placed back into the email. False detections or large delays: Support request can be made to attempt to speed up the process.

support@corvidcd.com | support.corvidcd.com | 800.349.2549

CORVID CYBERDEFENSE

Impersonation Protection

What it is: Impersonation Protection is designed to look for attacks that utilize similar domains, names, and/or come from known bad addresses.

What to expect: Outside the obvious of reducing the noise, policies can be created to prevent domain name social engineering attacks amongst other things. Each rule will need some TLC to prevent falsely blocking of personal email addresses, however the use of personal emails to company emails is questionable based on the lack of security.

Spam Detection

What it is: As an additional feature, Mimecast can provide Spam Detection. Actions on these events are to either add a spam ID in the subject line or to go as far as block the spam detected emails.

What to expect: If blocking has been requested, once an hour a digest email will be sent with a summary of the detections. It is recommended that subject tagging be the action taken to prevent legitimate emails from being held and needing to be released via the digest email or the Mimecast plugin. False detection: emails can be released from the digest email, the Mimecast plugin, or the Mimecast online portal.

Malware Detection

What it is: The malware policies look for known malware or macros (i.e. programming code).

What to expect: If malware is detected it will be quarantined. Macro management will need to be determined prior to implementing this feature to prevent false impact for clients that use macros within their organization. False detections: Macros are the only area within this policy where bypasses can be created.

URL Analysis

What it is: URLs within phishing emails are the number one threat to any organization. Mimecast will analyze all URLs within the email as well as attachments to determine if they are malicious. If deemed malicious, once the link is clicked, the action will be blocked and the Corvid Cyberdefense SOC (security operations center) will be notified.

What to expect: All URLs the user sees are "rewritten" to a Mimecast URL to allow for security checking. False detection: In some cases a URL that a user deems legitimate may be blocked because the destination website has been compromised. In this case, submitting a support ticket will prompt a review and the Corvid Cyberdefense SOC can assist to gain access as needed.