Mimecast Additional Email Security Features

05/07/2024 3:47 pm EDT

Here you will find some information about Mimecast's Email Features.

In addition to the default Mimecast Spam Security, additional email security policies will be applied for security and/or awareness.

1. **[External] banner appended to email body –** For every email that is received from an external source (from a domain other than your firm), a banner will be appended to the top of the email body. This policy is intended to remind the user to be more vigilant about the emails from outside the organization.

2. **URL Protection** – Once a link embedded in an email is clicked, the link will be filtered through Mimecast URL protection to ensure that the link is not harmful. Mimecast maintains and regularly updates the list of harmful sites in real time. Users will notice that links clicked in email will first filter through Mimecast before resolving to the webpage. This is to protect the user environment from unwanted/malicious sites. This typically only takes a few seconds.

3. **Impersonation Protection** – Mimecast will review and flag emails that are potential attempts to impersonate specific individuals in the organization to request money, usernames, password, gift cards, etc.

4. **Attachment Sandboxing Protection –** For every email that is received with attachments, Mimecast will strip out all attachments, scan them and open the attachments in a sandbox environment to ensure they do not contain and/or execute any malicious code. If nothing is found, the message will continue to the recipient. Should Mimecast flag any of the attachments as dangerous, it will be quarantined.

Need More Help? Click Here!