Weill Cornell Medicine

11.14

Email Security

Responsible Executive: Chief Information Officer, Weill Cornell Medicine
Original Issued: August 17, 2015
Last Updated: March 29, 2016
Last Reviewed: August 29, 2023

Contents

Policy Statement

All members of the Weill Cornell Medicine community are responsible for protecting the confidentiality, integrity, and availability of data created, received, stored, transmitted, or otherwise used by Weill Cornell Medicine.

Weill Cornell Medicine reserves the right to restrict the use of information technology resources in order to preserve data security or comply with law or policy.

In order to further secure Weill Cornell Medicine data and members of Weill Cornell Medicine, an institution-wide email security system has been implemented that incorporates spam filtering, advanced threat protection, and threat classification.

Reason for Policy

Email is a common method of both annoyance as well as data exfiltration, namely by the use of spam or phishing campaigns that may trick individuals into providing sensitive information to unauthorized parties. In order to protect against these threats, Weill Cornell Medicine has implemented an email security solution that is modular in nature and robust in terms of its capabilities.

Entities Affected by this Policy

All units of Weill Cornell Medicine, including Weill Cornell Medicine-Qatar.

Who Should Read this Policy

All members of the Weill Cornell Medicine community utilizing Weill Cornell Medicine information technology resources. All stewards and custodians of Weill Cornell Medicine data.

Web Address of this Policy

https://its.weill.cornell.edu/policies/

Contacts

Direct any questions about this policy, 11.14 – Email Security, to Brian J. Tschinkel, Information Security Officer, using one of the methods below:

- Office: (646) 962-2768
- Email: brt2008@med.cornell.edu

1. Overview

Weill Cornell Medicine has implemented an email security solution that provides spam message filtering and protection against security threats by blocking junk mail, spoofing attempts, and suspicious or malicious hyperlinks and attachments.

2. System Basics

The spam management feature is an email filtering tool; all incoming email is filtered by an anti-spam and anti-virus product. Messages are scored and thresholds have been set in alignment with industry standards and Weill Cornell Medicine's needs in order to safely quarantine messages that contain spam or malicious content. These thresholds are tuned in response to environmental changes and individual feedback.

The system also provides attack protection against suspicious or malicious hyperlinks and attachments. Hyperlinks are assessed for the likelihood of a threat or attack and rewritten in such a way to help protect individuals from accidentally clicking through and exposing themselves to an attack.

Attachments are securely screened and tested for the presence of suspicious or malicious code. Email messages found to contain such attachments are blocked from delivery in order to prevent infection or spread of malware such as ransomware. The delivery of emails containing attachments from external senders may be delayed on average three to five minutes, although the maximum delivery delay may take significantly longer depending on various technical circumstances.

Lastly, the email security system implements filtering of "spoofed" messages. Spoofed messages are often used by attackers to impersonate another individual in order to conduct a social engineering attack, typically to request monies or privileged credentials. The email system is configured to detect and quarantine messages that are spoofed. Quarantined messages will appear in the daily message digest or be outright blocked depending on various technical circumstances. False positives can be reported to ITS for investigation and allowlisting.

3. Individual Responsibilities

In order to help protect against email threats, all individuals are automatically enrolled in the email security solution. While individuals may tune some of the spam filtering and digest features, they cannot withdraw from the provided security features due to the resulting security implications.

3.01 Assistance with Email Security System

Individuals that are experiencing technical difficulties with the email security system should contact ITS for assistance. A Spam Management System FAQ is available for assistance with common issues and questions.

If too many messages are being incorrectly filtered, individuals can adjust their quarantine, Safe Senders List, and Blocked Senders List options. ITS can assist individuals learning how to manage these controls.

3.01.001 Decoding Hyperlinks

The system is equipped with a target attack protection algorithm that rewrites hyperlinks contained in email messages in order to lessen the risk of clicking on something malicious. ITS recognizes there may be a legitimate business need to retrieve the original, unaltered hyperlink. Individuals can "decode" the hyperlinks contained in email messages by copying the hyperlink into the Proofpoint URL Decoder (https://decode.weill.cornell.edu).

3.02 Message Digest Delivery

By default, a summary digest of all quarantined messages is delivered to the individual's mailbox twice daily at approximately 8:00 AM and 6:00 PM Eastern Time. Digests include a list of any messages that may have been quarantined since the previous digest was delivered. In the event no messages are quarantined, a digest is not delivered.

Individuals who wish to receive digests on a different frequency may request to switch to a once daily digest, delivered at approximately 12:00 AM ET. Individuals who do not wish to receive any digests may withdraw by deselecting the checkbox in their Profile settings of the web portal (https://antispam.med.cornell.edu). Individuals who choose to withdraw from a digest completely will be responsible for manually accessing the Proofpoint web console to check the quarantine at-will.

Requests to switch digest delivery options may be submitted by the individual as an ITS Support ticket.

3.02.001 Option 1: Less Restrictive Spam Filtering

Individuals that appreciate the use of the spam filtering but find that too many messages are not being delivered and flagged inadvertently may opt to switch to a less restrictive policy. ITS has created a “moderate” policy with a lesser quarantine score which may increase the number of messages reaching the individual’s mailbox. This policy allows individuals to receive emails automatically classified as “bulk” messages, which typically consist of mass mailings, newsletters, and other commercial email. It is important to note that suspicious or malicious messages may be incorrectly automatically classified as “bulk” messages and delivered to the individual’s mailbox without proper filtering. Consequently, individuals opting for less restrictive spam filtering may need to be on heightened alert for messages with suspicious or malicious hyperlinks or attachments.

Requests to switch to the less restrictive spam filtering policy may be submitted by the individual as an ITS Support ticket.

3.02.002 Option 2: Withdraw from Spam Filtering

Individuals who wish to withdraw from spam message filtering altogether may experience an extreme excess in the amount of email messages that are delivered to their mailbox (as opposed to being filtered and quarantined by the system). This policy allows individuals to receive emails automatically classified as “bulk” and “spam.” If withdrawing from spam message filtering, the security features (anti-virus scan, hyperlink protection) will still remain in effect. It is important to note that suspicious or malicious messages may be incorrectly automatically classified as “bulk” or “spam” messages and delivered to the individual’s mailbox without proper filtering. Consequently, individuals opting for less restrictive spam filtering may need to be on heightened alert for messages with suspicious or malicious hyperlinks or attachments.

By withdrawing from spam message filtering altogether, individuals will be responsible for managing the excess email on their own.

Please note, as defined in ITS policy 11.08 – Use of Email, forwarding to a non-ITS managed third-party filter or email system will not be permitted.

Requests to withdraw from spam filtering may be submitted by the individual as an ITS Support ticket.

4. Additional Resources

The following additional resources are available:

- Spam Management System FAQ
- Weill Cornell Medicine Anti-Spam Portal

Revision History:

Date	Author	Revision
August 17, 2015	Brian J. Tschinkel	Policy implemented
March 29, 2016	Brian J. Tschinkel	Added attachment scanning features
August 13, 2022	Justin Barber	Updated Individual Responsibilities
August 29, 2023	Brian J. Tschinkel	Updated policy template and language to conform with branding