Weill Cornell Medicine

11.14

Email Security

Responsible Executive: Chief Information Officer, WCM
Original Issued: August 17, 2015
Last Updated: March 29, 2016

Policy Statement

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

WCM 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 WCM data and members of WCM, WCM has implemented an institution-wide email security system that incorporates spam filtering, advanced threat protection, and threat classification.

Reason for Policy

Email is a common method of data exfiltration, namely by the use of spam messaging and phishing campaigns in order to trick users into providing sensitive information on a fake website. In order to protect against these advanced persistent threats, WCM has implemented an email security solution that is modular in nature and robust in terms of its capabilities.

Entities Affected by this Policy

Weill Cornell Medicine

Who Should Read this Policy

All employees, faculty, students, and affiliates of Weill Cornell Medicine

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

Contents

1. Overview

WCM has implemented an email security solution provided by Proofpoint. The system provides spam message filtering and protection against advanced persistent threats by blocking spoofing attempts, intercepting malicious hyperlinks, and scanning attachments in email messages that may contain malicious code.

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 WCM needs in order to safely quarantine messages that contain spam or malicious content. These thresholds are tuned regularly in response to environmental changes and user feedback.

The system also provides targeted attack protection against malicious hyperlinks and attachments contained in email messages. Hyperlinks are assessed for the likelihood of a threat or attack. Hyperlinks are rewritten in such a way to protect end users from accidentally clicking through and exposing themselves to an attack or infection.

Attachments are securely screened and tested for the presence of malicious code, or “sandboxed.” Email messages found to contain malicious attachments are blocked from delivery in order to prevent infection or spread of ransomware. The delivery of emails containing attachments from external senders may be delayed on average 3 – 5 minutes, although the maximum delivery delay will not exceed 15 minutes.

Lastly, the email security system implements filtering of “spoofed” messages. Spoofed messages are often used by attackers to impersonate another user 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. False positives can be reported to ITS for investigation and whitelisting.

The implementation of this system has shown a dramatic increase in the number of spam-related messages that have been quarantined and a decrease in the amount of compromised user accounts by protecting malicious hyperlinks and attachments. As this system provides an adequate layer of defense against malicious attacks both on and off the WCM network, all individuals with a WCM email account are automatically enrolled in these services for free.

3. Individual Responsibilities

In order to ensure all individuals are protected against threats through the WCM email system, all users are automatically enrolled in the spam filtering and security features (anti-virus scan, hyperlink protection, attachment scanning and testing, anti-spoofing) of the email security solution. Due to the security implications that may occur from withdrawing from these services, users may tune some of the spam filtering and digest features, but may not withdraw from the provided security features.

3.01 Assistance with Email Security System

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

If too many messages are being blocked inadvertently, users can adjust the quarantine, white list, and black list options. ITS Support can assist users learning how to manage these controls. Additional options are available below.

3.01.001 Decoding Hyperlinks

The system is equipped with an advanced 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 in order to retrieve the original, unaltered hyperlink. Users can “decode” the hyperlinks contained in email messages by copying the hyperlink into the Proofpoint URL Decoder (https://decode.weill.cornell.edu). As this system is still under development, feedback can be submitted to ITS Support for consideration for further enhancements.

3.02 Message Digest Delivery

By default, a summary digest of all quarantined messages is delivered to the user'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 the Profile settings of the web portal (https://antispam.med.cornell.edu). Individuals who choose to withdraw from a digest completely will be responsible for 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 improve the reliability of legitimate messages reaching the user's mailbox. This policy does not block bulk messages, which typically consist of mass mailings, newsletters, and other commercial email.

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 may experience an extreme excess in the amount of email messages that are delivered to their Inbox (as opposed to being filtered and quarantined by the system). By withdrawing from spam message filtering, users will be responsible for managing the excess email on their own. Please note, as defined in ITS 11.08 – Use of Email, forwarding to a non-ITS managed third-party filter or email system will not be permitted.

If withdrawing from just spam message filtering, the security features (anti-virus scan, hyperlink protection) will still remain in effect as this does not increase the likelihood of a security attack.

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
- WCM Spam Portal

5. Definitions

These definitions apply to institutions and regulations as they are used in this policy. Definitions of technical terms are supplied by NIST IR 7298 Revision 2, *Glossary of Key Information Security Terms*.

- WCM — Weill Cornell Medicine
- ITS — Information Technologies & Services Department
- spam — The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

- phishing — Tricking individuals into disclosing sensitive personal information through deceptive computer-based means.
- spoofing — Faking the sending address of an email message in order to deliberately induce a user to take incorrect action, usually through the use of spam or phishing.
- ransomware — Type of malicious software (or “malware”) that restricts access to the infected system (or other interconnected systems) in some way and demands that the user pays a ransom to the attackers in order to remove the infection. In most cases, this type of infection is spread via malicious email attachments.
- APT — Advanced Persistent Threats. An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders’ efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.