Sender Policy Framework (SPF)

Overview

There are times when emails may be blocked due to an issue with the email's domain. In this case, the SPAM filter will not automatically release these email(s). The email sender must correct the Sender Policy Framework (SPF), with their email domain, in order for the issue to be resolved. A detailed explanation of why these emails are blocked is outlined below.

Why are the emails blocked?

The McLennan Community College (MCC) Information Systems and Services (ISS) Infrastructure team has acted to raise our cybersecurity posture regarding incoming email messages. The first action is the filtering of email messages that fail Request for Comments (RFC) 7208 Sender Policy Framework (SPF). The second action taken is the filtering of email messages from domains with no published SPF record.

Initially, these messages will be quarantined. Quarantining the messages provides the MCC recipient the opportunity to review the affected message and release for delivery, if the MCC employee feels safe to do so. Additionally, quarantining the messages allows MCC employees and the ISS Infrastructure team to identify MCC partners and vendors not compliant with RFC 7208 and work with them to bring into compliance.

When MCC partners are identified to be out of compliance with RFC 7208, the ISS Infrastructure team will make every effort to assist the partner in configuring their email domain to be compliant. When outside vendors are identified to be out of compliance, by MCC staff, ISS Infrastructure members will provide our policy with the MCC staff member to share with non-complaint vendors and direct them to resources to assist them with becoming compliant.

Sender Policy Framework (SPF) Explained

We have come to a time and place where relaxed cybersecurity standards can have grave financial consequences for all. When a domain owner does not publish an SPF record, they leave their domain open for fraudulent use. Sometimes fraudulent emails are sent to their partners, changing money transfer details at the last minute, which redirect large sums of money into the accounts of the fraudsters. In this scenario both the sending and the receiving domain owners fall victim to the fraud.

Often, domain owners are unaware their domain name is being used fraudulently. When a domain’s email identity is used fraudulently, or spoofed, the online reputation of that domain is diminished. Typically, domain owners only become aware of the fraudulent use after their own legitimate emails are rejected by email domains, with SPAM filters in place, or where a large sum of money is unaccounted. At this time, system administrators are required to spend hours repairing their domain's online reputation, going through checks, to show the major email providers, they have eliminated the fraudulent use and their domain name may be removed from the list of fraudulent email senders. During this remediation period, conducting business for the organization becomes more difficult, due to the fact their emails are being rejected by most major email providers.

The Sender policy framework (SPF) was established as a tool for domain owners to guard against the fraudulent use of their domain name and protect their online reputation. When domain owners publish a properly formatted SPF record, they authoritatively declare the legitimate source(s) of emails sent from their domain. When an email passes a receiving domain’s SPAM filter SPF checks, they know the email, from the sending domain, is safe to accept.

Last updated: 5/4/23

Revision #1
Created 22 November 2024 18:41:34 by Laura J. Crapps
Updated 22 November 2024 18:47:51 by Laura J. Crapps