Why is McAfee blocking valid emails?

Author:
Webservio Inc.

Created On: 06 Dec 2013 10:12 AM

McAfee SaaS Email Protection service will block (or quarantine depending upon service settings) any mail that scores as â€œprobable spamâ€• unless that senderâ€™s domain or e-mail address is on one of the available Sender Allow Lists within the service â€“ either domain or user-level.
Â
In some cases email from an otherwise trusted sender may be blocked with a variation of a 554 error or quarantined.
Â
If a sender receives a 554 error on a message that is being sent directly to a McAfee SaaS customer (not a reply or a forwarded message), it is probable that the sending domain or IP address has been â€œfingerprintedâ€• based on recent sending habits.
Â
Many times, upon investigation, it is found that *someone* from the sending domain has sent a recent email that met one or more of the following criteria that increased the spam score in our spam detection system.
Â
- A percentage of messages were sent to invalid recipients generating a large number of NDRs. Typically when this is seen, it is taken as a possible directory harvest attack and the spam score elevates accordingly
Â
- Messages sent were received by â€œhoneypotsâ€•. Honeypots â€“ or spam traps â€“ are trusted servers around the world set up with dummy e-mail addresses that sit and wait for mail to hit. Mail hitting these servers is automatically classified as spam because the accounts tied to these servers have not been advertised or requested mail. Any mail sent is deemed unsolicited and therefore spam. Again, this is common with directory harvest attacks and the spam score of messages sent from that domain will be elevated accordingly
Â
- Messages that were sent from the sending domain may have been reported by the recipient to their ISP as potential spam. These complaints are reported through various sources and aggregated in the spam score of all inbound messages through the SaaS Email Protection service and may affect the score enough to have the mail either quarantined or blocked. This typically will come about if the sender is not using opt-out links and/or not honoring opt-out links in certain types of messages being sent from their domain