554 5.7.1 Delivery not authorized

554 5.7.1 Delivery not authorized

Question

I tried to send MIT email and got an email error "554 5.7.1", what does it mean?

> *554 5.7.1 Delivery not authorized*
> *554 5.7.1 You are not allowed to connect*

Answer

It probably means that MIT's spam filter blocked the mail.

Knowing why the mail was blocked is harder - our spam filter can block various messages for various reasons.

Microsoft's official answer to the topic is here:
https://answers.microsoft.com/en-us/msoffice/forum/all/email-sent-through-smtp-smtpoffice365com-is-being/9b2b700a-cafc-4524-a50e-c6dce61db
- Message Rejected with SMTP Code 554. 5.7.1

MIT-specific answer

While Microsoft's official answer gives a few bullet points for people to work through, we will comment that the most common situations encountered by IS&T Customer Support are:

- problems with the sender's reputation
- problems with the sender's DNS.

Sender's Reputation

When a sending site connects to MIT to submit mail, MIT's spam filter does some lookups based on the IP address of the connecting site. If the spam filter determines that the sender's IP address has a "negative reputation", it will reject the mail with a 554 5.7.1 error.

To investigate problems with the sender's reputation, consult
http://ipremoval.sms.symantec.com/lookup/

Sender's DNS

In addition to considering the reputation of the sender's IP address, MIT's spam filter also checks to see if the sender has configured reverse DNS for their IP address. Loosely speaking, MIT requires that the sender have a properly-configured hostname, and treats them as a spammer if they do not.

The message "Delivery not authorized" could happen for multiple reasons:

- no reverse DNS record exists for the connecting IP address
- the reverse DNS record exists for the connecting IP address, but the 'A' or 'AAAA' record of the resulting domain does not match the connecting IP address
- the domain provided at HELO and EHLO has neither an 'A', nor an 'AAAA', nor an 'MX' record in DNS

Other considerations

The most important question to start with is "when the sending site contacts MIT, what IP address does MIT see?" Reputation and DNS lookups start with the IP address.

Unfortunately, mail errors do not always give a good report of IP addresses. The sender may not know the IP address of their edge mail servers.

One approach is to ask the sender to send a test message to a non-MIT site like Gmail. Once the test message is received, we can use "show

original" to view the Received headers, which will reveal IP addresses of mail servers.

How to check DNS

You can use `nslookup` or `host` or other tools to check to see if an IP address reverse-resolves.

examle of using "host" to do reverse-DNS lookup
$ **host 18.70.0.160** 160.0.70.18.in-addr.arpa domain name pointer W20NS.MIT.EDU.