Email box

PARTNER UPDATE – April 20th, 2021

Hello Valued Customers,

"I started getting a bounce every time I email a mailbox in my organization, yet my coworker is receiving the emails!"

Have you ever run into this at your organization? I receive queries from or clients on this weekly. In fact, this email is derived for just such a query I receive only this morning. Whenever someone at this client's office sent out an all-hands email, the sender would receive a bounce from my test mailbox, dpowell@XXXXXX.com (not the real email address!).

Let's dig into this together. The mailbox dpowell@XXXXXX.com has a forwarding rule to send any received email messages to my company mailbox. That way any alerts I had set up to be sent to my client-domain email box would reach me at our office. Sometime after this was set up, Microsoft made a policy change. The change was to deny external forwarding by default, as this is an often-used data exfiltration method. This is certainly not to say that everyone who forwards mail to another outside account is a scoundrel stealing company data. Rather that scoundrels stealing company data did use this tactic. It is a favorite tactic of phishing scams and can go on undetected for long periods.

So, in an overabundance of caution, Microsoft disabled this behavior as the default policy. Now, if you want to forward email outside the organization you must specifically allow this behavior. You can enable this on an individual basis through the spam rules. The way that this issue and others like it can be decoded is available in the message that you received in the bounce message. These usually contain a code that gives the reason for the bounce. In this case here is the giveaway:

```
Diagnostic information for administrators:
Generating server: XXXXXXXXXXXXX.namprd17.prod.outlook.com
dpowell@XXXXXX.com
Remote Server returned '550 5.7.520 Access denied, Your organization does not allow
external forwarding. Please contact your administrator for further assistance. AS(7555)'
Original message headers:
Received: from XXXXXXXXXXXXX.namprd17.prod.outlook.com (2603:10b6:a03:379::7)
  by XXXXXXXXXXXXX.namprd17.prod.outlook.com (2603:10b6:a03:29d::21) with
  Microsoft SMTP Server (version=TLS1_2,
  cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.4042.16; Wed, 14 Apr
  2021 18:42:00 +0000
```

A google search of the highlighted text returns as one of the top results a Microsoft article describing the issue and how to resolve:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/external-email-forwarding?view=o365-worldwide

If you read this article you will come across the paragraph that contains the 'secret-sauce' of the resolution: For instructions on how to configure these settings, see Configure outbound spam filtering in EOP.

If you follow the instruction at this anchor in the above referenced article you will be able to allow this behavior on an individual basis at your organization.

The real magic here is not how to fix this particular issue, but instead how to use the information provided inside the bounce message to decode the problem and find a solution. Now not all bounce messages will have as straight forward of a cause, and sometimes you might have to try though multiple possible solutions till one works for you. But you can be assured the bounce message itself is always your best hint.

Now if you run into an issue that proves difficult to resolve as always you can call the KIS helpdesk at (510) 403-7500 and one of our expediters will get an engineer scheduled to help you resolve it. And if you are new to KIS, our expediters explain our rates and get you set up.

David

David Powell
Partner & Director of Cloud Service / VMware Advanced Systems
KIS - Keep IT Simple | Professional IT Solutions Experts Since 1988
E: powell@kiscc.com
O: (510) 403-7500