Security

What are the password security policies available on Mithi SkyConnect?

Password complexity can be defined and enforced e.g. password should have 3 alphabets, 2 numeric characters and 1 special character. Minimum Password length can be specified. Password age can be defined. After which it will expire and force the users to reset their password. Password history can also be defined to dissuade users from reusing recent passwords.

In our environment, users sometimes need to share their credit card numbers in the email. At no point this information should be available to anyone working on the server (not even in logs). How does Mithi ensure this content security in Mithi SkyConnect?

The solution components do not store any part of the message body in any of the logs. This will ensure that no part of the message is visible in the logs. Only the subjects are stored for troubleshooting and reporting. The only place the mail is delivered in its entirety is to the user's inbox and to the archival system (if configured). If you plan to host your domains on our cloud setup, you may want to read more about the measures we have put in place to secure access to your data. For more information refer the links Mithi SkyConnect SLA

Can we disable mobile access for certain set of users in SkyConnect?

SkyConnect supports standard protocols for services, which are used by the clients, both desktop and mobile. Since the last mile connection to the services happen over the same protocols, irrespective of where the connection comes from (desktop, mobile or web), it is not possible to enforce a policy for disabling mobile access for certain users.

The workaround to this is to allow such users only web client access and disable their POP/IMAP completely. This will ensure that these users cannot access their mail neither from mobile nor from desktop clients like Thunderbird or MS Outlook.
User set 1: Web client access only, no mobile, no desktop client access
User set 2: Web client access, mobile access, desktop client access
User set 3: No Web client access, mobile access, desktop client access.

Can SkyConnect control mail from legitimate ids which masquerade someone else?

Situation

A user of our customer's domain, received a mail from his chairman, with some instructions. The user responded to the email with the required information, before realizing that the mail was actually not from the chairman.

Observation

While the name of the sender was the same as chairman's name, the email id was a public email id. So technically it's a legitimate email from valid email id. The display name can be set to anything.

Simply speaking, there can be multiple people in the world, with the same name.

So while this is a spoof email, it cannot be detected as one by most or all email security scanners.

E.g. "Ravi Khanna".

Most email clients simply show the display name, when you read the email. So it may be misleading.

We confirmed the following:

1. Mithi SkyConnect is running ATP (advanced threat protection) and uses sand-boxing to filter malware.

2. The mail system is checking SPF, DKIM, DMARC of inbound email traffic to identify rogue or spam email, based on the email id (and not the display name)

3. In this case, the email is a legitimate email from a public email service, with a display name matching a person in our customer's organization. So actually this is not a spoof mail at all. It's simply a mail from a person whose name matches the name of one of the employees of the company. This is perfectly legit and cannot be blocked at any level.

Our recommendation

1. Build awareness among the user community to be more aware before responding to an email asking for personal information, financial information and other classified information. This should be done on an ongoing basis using

classrooms, videos, FAQs, and email alerts.

2. Report the mail as abuse on the sending platform, so they can take appropriate action

3. We propose that you also report this to the local cyber-crime unit of your region, so they can ask the public email id provider or the sender's IT team for more information to locate the user via the IP address.

4. Put in a filter on the inbound mail scanner to insert a message for mail coming from external domains to alert the users.

Remember, the human is the weakest link in any security chain.
