Task 4: Litigation Hold and Recovery Operation

Objective: To apply a litigation hold on a user's mailbox, simulate item deletion, and then recover the deleted items.

Instructions:

1. Apply a litigation hold on 'Andre Onana's' mailbox to safeguard against data loss.
2.Simulate an item deletion scenario within his mailbox.
3.Navigate the recovery process and restore the deleted items.

Implementation Steps

1. Apply a litigation hold on 'Andre Onana's' mailbox to safeguard against data loss.

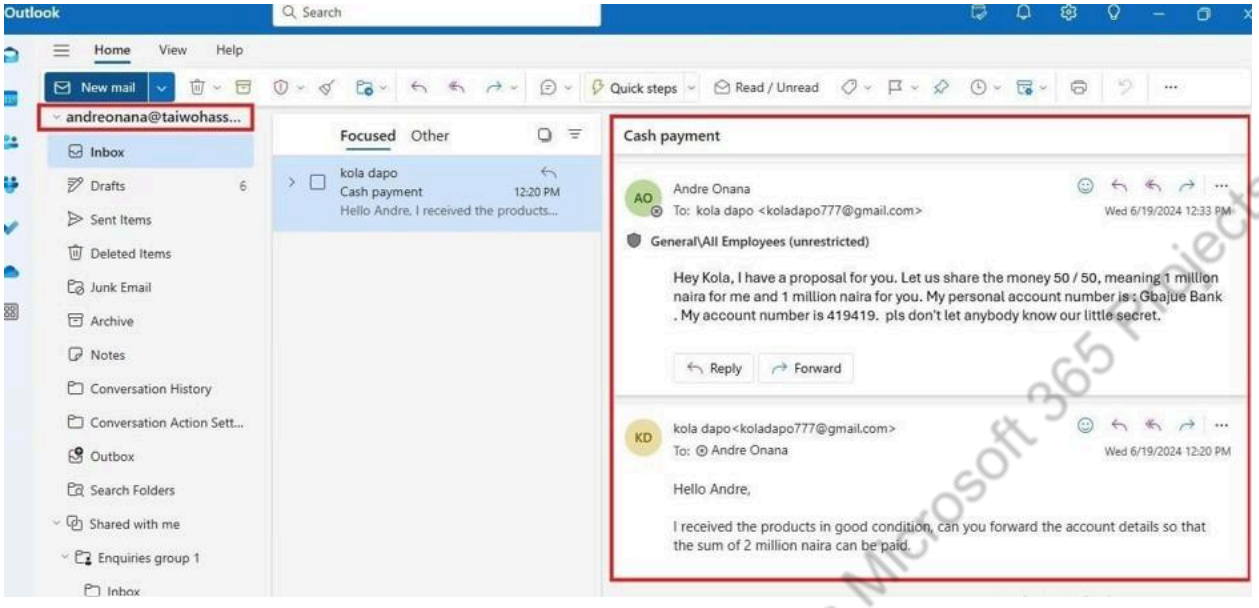
   Step 1: Displays a simulated fraudulent email exchange in Andre Onana's Outlook account with an external supplier named 'Kola Dapo'.

   Access Andre Onana's Outlook Account: Andre Onana (or I, if performing the simulation) logged into Andre Onana's Outlook client or Outlook on the web.

   Compose and Send Simulated Fraudulent Email: From Andre Onana's account, I composed a new email addressed to 'Kola Dapo' (an external supplier). The email was crafted to simulate a fraudulent activity, for instance, by discussing a payment or order under suspicious pretences.

   Receive Reply from Simulated External Supplier: A reply from 'Kola Dapo' was sent back to Andre Onana, completing the simulated fraudulent exchange.

   Observe Email in Inbox/Sent Items: The screenshot captures Andre Onana's Inbox, showing the received fraudulent email from 'Kola Dapo' with the subject "RE: Important - Urgent Payment Inquiry". This visual evidence confirms the successful simulation of the fraudulent mail activity, which is a prerequisite for demonstrating the effectiveness of a litigation hold shown in the Screenshot below.



Fraudulent mail exchange between Andre Onana and a supplier named “Kola Dapo”

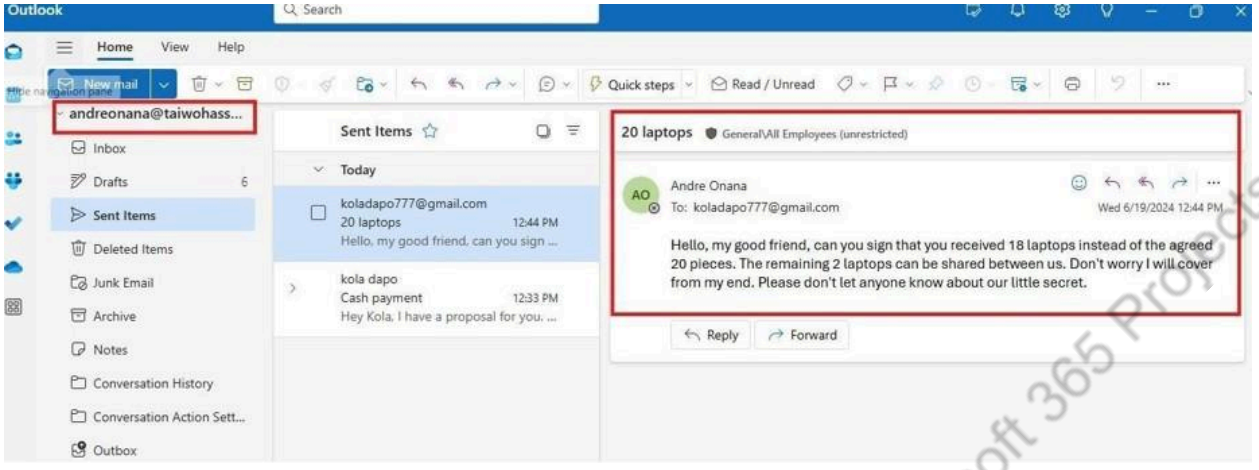
Step 2: Displays a second simulated fraudulent email exchange in Andre Onana's Outlook account, this time involving a "customer on Laptops" named 'Kola Dapo'.

Access Andre Onana's Outlook Account: Andre Onana (or I, if performing the simulation) logged into Andre Onana's Outlook client or Outlook on the web.

Compose and Send Second Simulated Fraudulent Email: From Andre Onana's account, I composed a new email, this time addressed to 'Kola Dapo' (the simulated customer on Laptops). The email was crafted to continue the simulation of fraudulent activity, as evidenced by the subject "Re: Urgent Laptop order confirmation".

Receive Reply from Simulated Customer: A reply from 'Kola Dapo' was sent back to Andre Onana, completing this second simulated fraudulent exchange.

Observe Email in Inbox/Sent Items: The screenshot below captures Andre Onana's Inbox, showing the received fraudulent email from 'Kola Dapo' with the subject "Re: Urgent Laptop order confirmation". This visual evidence confirms the successful simulation of another fraudulent mail activity within Andre Onana's mailbox, further setting the stage for demonstrating the litigation hold.



Screenshot showing another fraudulent mail exchange between and a customer about Laptops

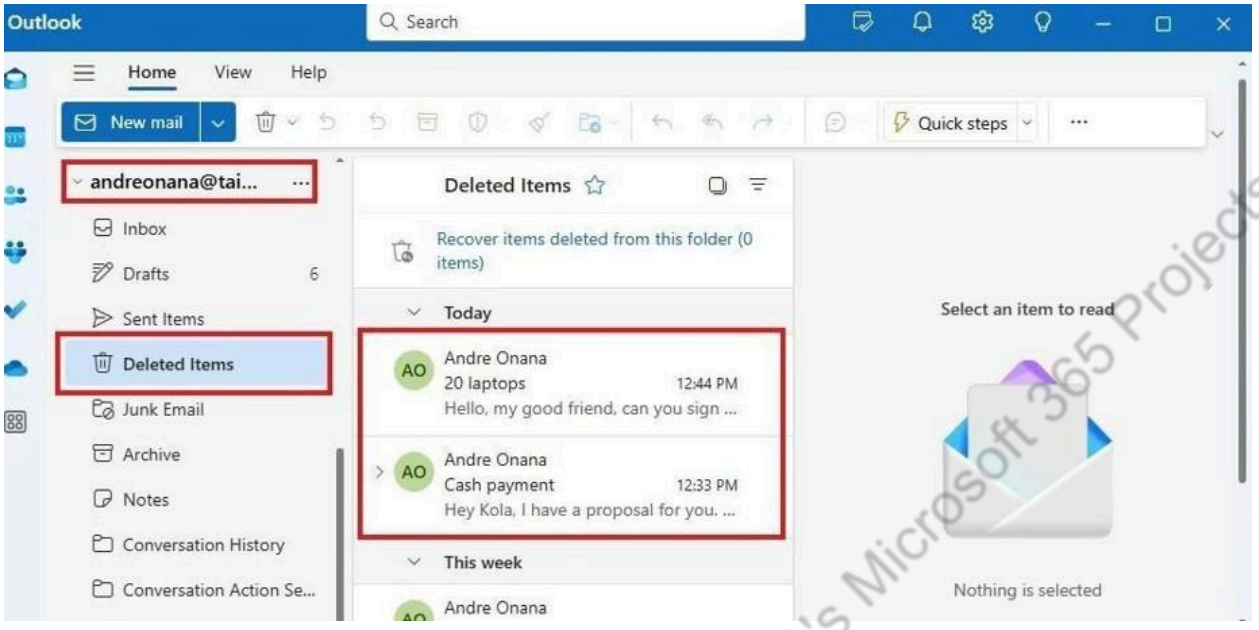
2. Simulate an item deletion scenario within his mailbox.

Step 1: Displays Andre Onana's Outlook account where he is attempting to delete previously received fraudulent emails.

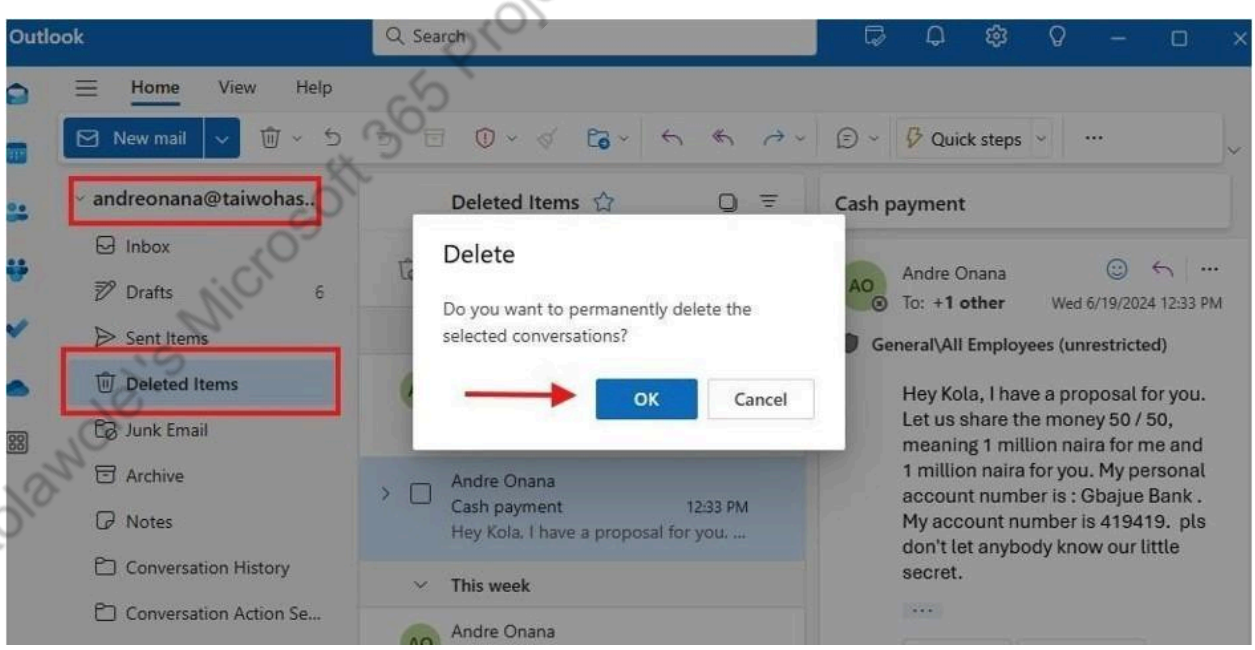
Access Andre Onana's Outlook Account: Andre Onana (or I, if performing the simulation) logged into Andre Onana's Outlook client or Outlook on the web.

Locate Fraudulent Emails: Within Andre Onana's Inbox, I located the fraudulent emails from 'Kola Dapo' (as previously simulated) about illicit cash and laptop transactions.

Initiate Deletion: Andre Onana (or I) selected these fraudulent emails. The screenshots specifically show the selected email from 'Kola Dapo' with the subject "RE: Important - Urgent Payment Inquiry" and the "Delete" button highlighted, indicating an attempt to remove it from the Inbox. As shown in the Screenshots below.



Andre Onana went to delete both fraudulent emails from his Outlook Account



Andre Onana makes sure he permanently deletes fraudulent emails from his Outlook Account

3. Navigate the recovery process and restore the deleted items.

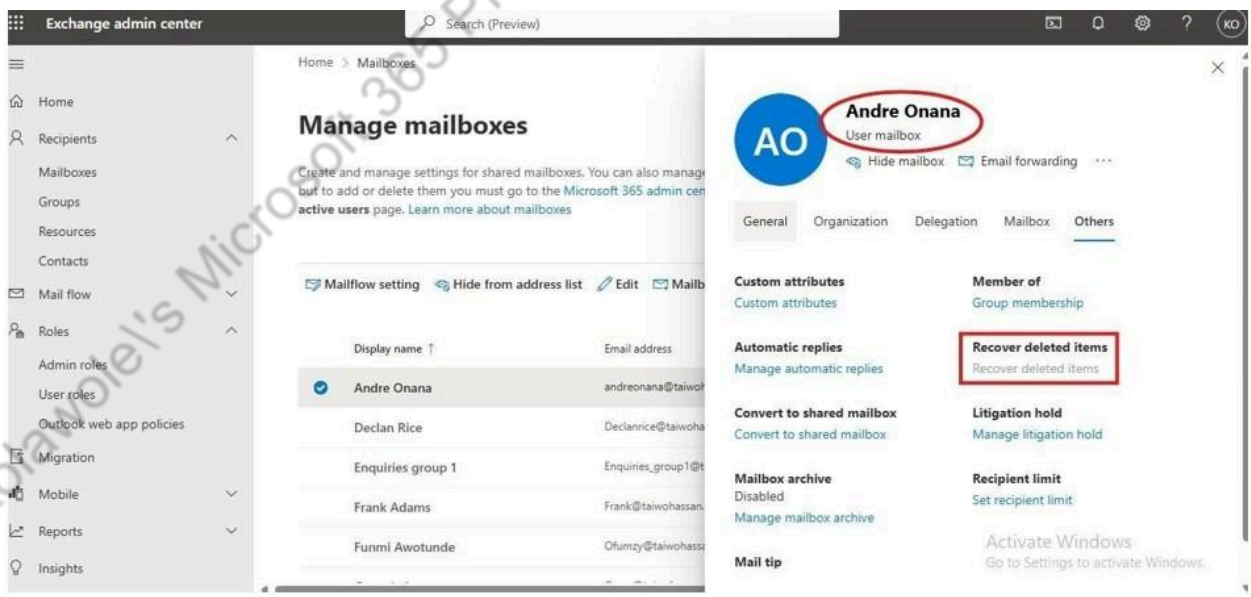
Step 1: Displays Andre Onana's mailbox properties in the Exchange admin centre, specifically highlighting a "greyed out" option related to deleted item recovery.

Accessed the Exchange Admin Centre (EAC): I logged in to the Microsoft 365 portal with my administrative credentials and navigated to the Exchange admin centre.

Located Andre Onana's Mailbox: In the EAC, I selected "Recipients" from the left-hand navigation pane, then clicked on "Mailboxes." I then searched for and selected 'Andre Onana's' mailbox from the list to view its properties.

Navigated to Recovery/Retention Settings: Within Andre Onana's mailbox properties, I would have navigated to a section related to recovery, retention, or general mailbox management where options for handling deleted items are present.

Observed Greyed Out "Recover deleted items" Button: This screenshot below captures the specific view where the "Recover deleted items" button or link appears, but is unclickable or "greyed out". This indicates that while the litigation hold might be in place, an additional configuration or permission might be required to enable the direct recovery function from this specific administrative interface, presenting a challenge that needs to be addressed before proceeding with the item recovery task.



Admin began recovery of deleted items, but me a greyed out button of “Recover deleted item”

Step 2: Displays the process of assigning the "Mailbox Import Export" role to allow for recovery of deleted items in the Exchange admin centre (EAC).

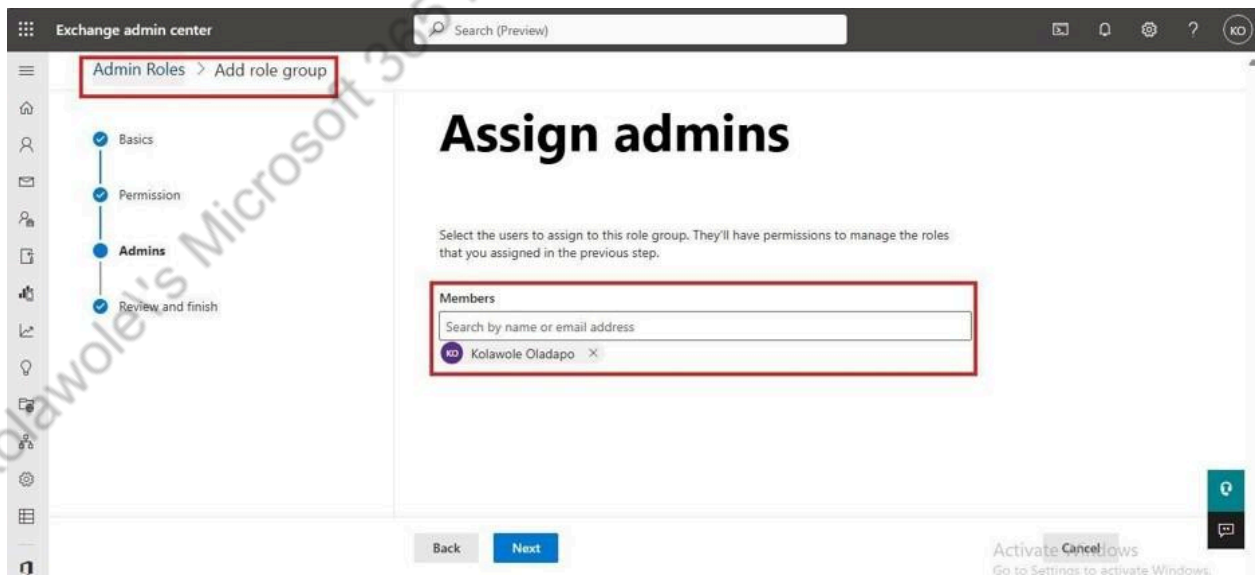
Navigated to Roles & Admins: In the EAC, from the left-hand navigation pane, I selected "Roles & Admins" (or "Permissions" in older versions) and then clicked on "Admin roles".

Selected a Role Group for Editing: I identified an existing role group or chose to create a new one to which I would add the necessary permission. The screenshot shows the "Organization Management" role group selected, indicating that I chose to modify this existing administrative group.

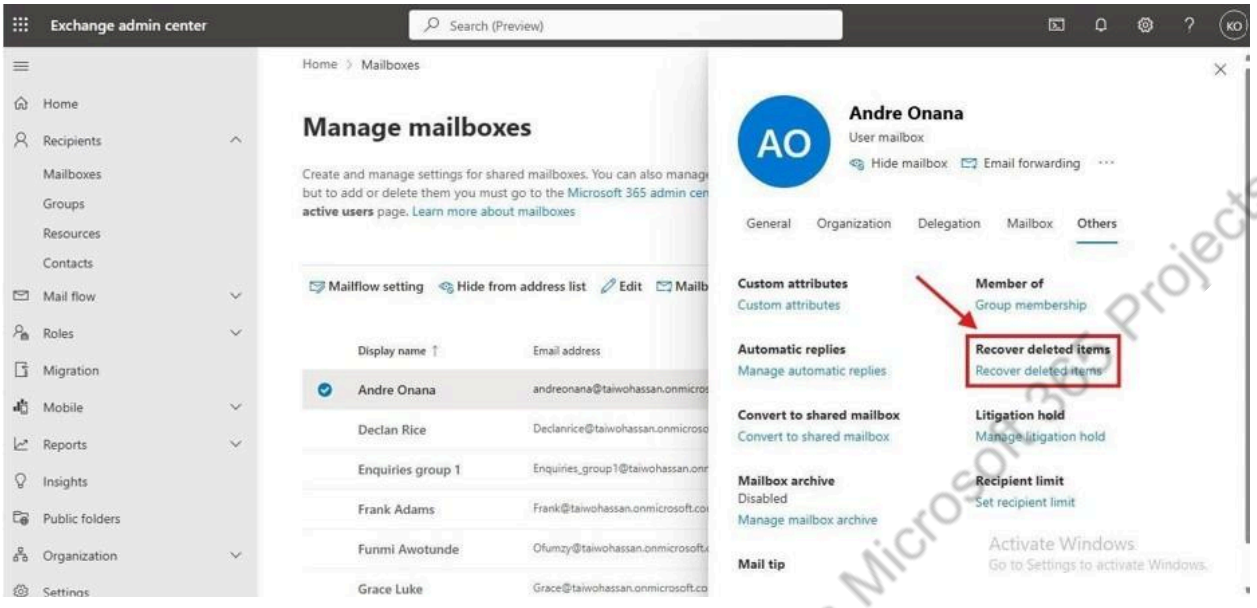
Edited Role Group Properties: I clicked on "Edit" or opened the properties of the selected role group.

Added "Mailbox Import Export" Role: Within the role group's properties, I navigated to the "Roles" section and clicked "Add role". From the list of available roles, I searched for and selected "Mailbox Import Export".

Saved Changes: After adding the role, I clicked "Save" or "Apply" to confirm the changes to the role group. This action granted the necessary permissions (including the ability to recover deleted items) to members of this role group, including myself, thereby resolving the "greyed out" button challenge. The successful action of the assigned “Mailbox Import Export” role shown in the first screenshot resulted in the second screenshot showing that the “Recover deleted items” is not greyed out anymore.



The Admin is assigned the “Mailbox Import Export” role



“Recover deleted items” button visible after Admin is assigned the “Mailbox Import Export” role

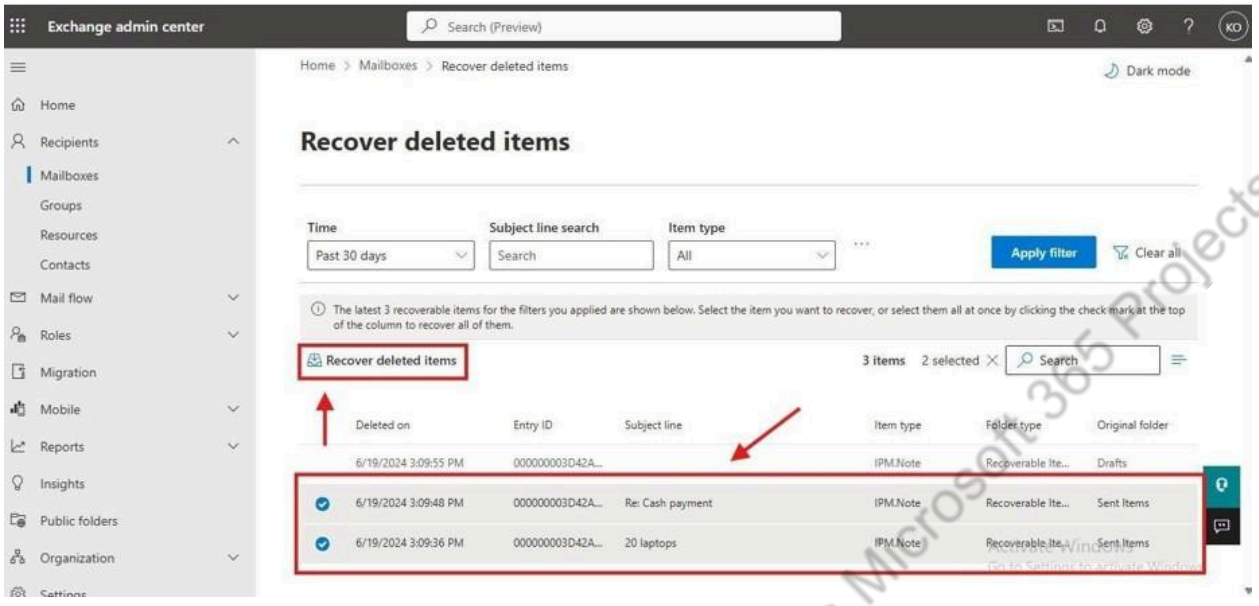
Step 3: Displays the recoverable items from Andre Onana's mailbox, specifically showing the previously deleted fraudulent emails, after gaining the necessary administrative permissions.

Located Andre Onana's Mailbox: In the EAC, I selected "Recipients" > "Mailboxes," then searched for and selected Andre Onana's mailbox.

Accessed Recovery Options: Within Andre Onana's mailbox properties, I navigated to the appropriate section for recovery or retention settings. After successfully assigning the "Mailbox Import Export" role (as per the previous step), the "Recover deleted items" button, which was previously greyed out, became active and accessible.

Initiated Deleted Item Recovery: I clicked on the now-active "Recover deleted items" button. This action opened a new interface or window, allowing me to view and select items that had been soft-deleted from Andre Onana's mailbox.

Viewed Recoverable Fraudulent Emails: The screenshot below clearly shows this recovery interface, displaying the previously deleted fraudulent emails, such as the one with the subject "RE: Important - Urgent Payment Inquiry" from 'Kola Dapo' and "Re: Urgent Laptop order confirmation" from 'Ahmed Taiwo'. This confirms that the litigation hold successfully preserved these items despite the user's deletion attempts, and my assigned role enabled me to access them for potential recovery.

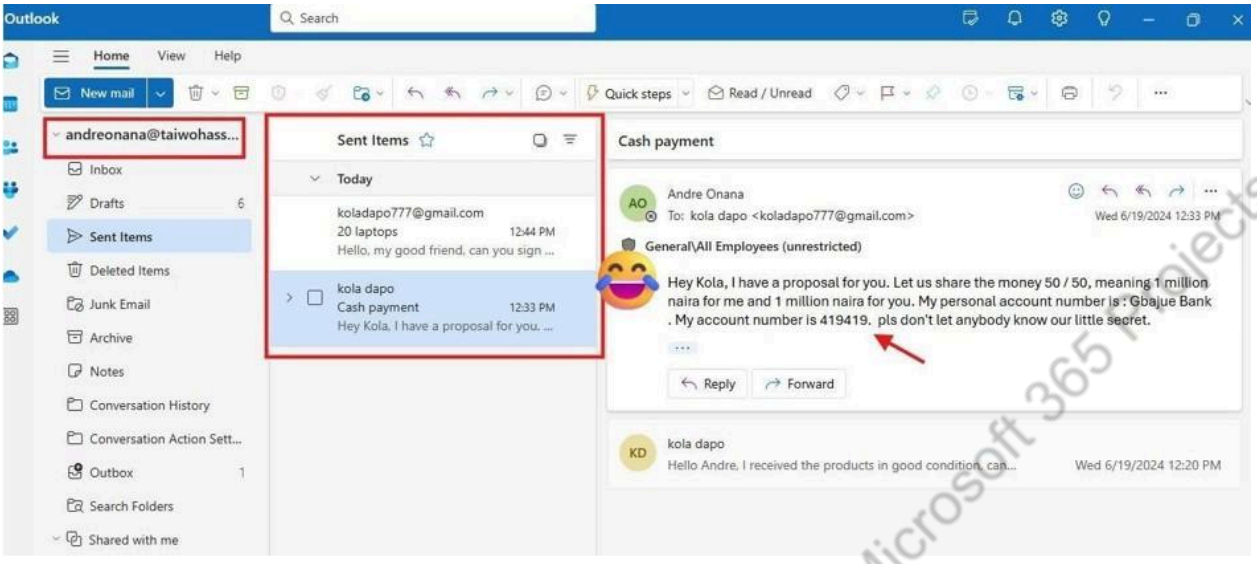


Admin detected and recovered the deleted fraudulent emails from Andre Onana's Outlook

Step 4: Displays the successfully recovered fraudulent emails now visible within Andre Onana's Outlook inbox, confirming the effectiveness of the litigation hold and the administrator's recovery actions.

Initiated Recovery of Deleted Items (Admin Console): Following the successful assignment of the "Mailbox Import Export" role, and with the "Recover deleted items" button now visible in the Exchange Admin Center (as shown in the previous step), I proceeded to select and initiate the recovery of the specific fraudulent emails from the recoverable items list.

Verified Recovered Emails in Outlook: After the recovery process was completed through the Exchange Admin Centre, the result is the screenshot below now clearly shows the previously deleted fraudulent emails, sent to and fro between "Andre Onana" and "Kola Dapo" with the subject "RE: Important - Urgent Payment Inquiry" and another with the subject "Re: Urgent Laptop order confirmation," now residing back in his Inbox. This visual confirmation demonstrates that the litigation hold successfully preserved the items, and I, as the admin, was able to recover them into the user's active mailbox, completing the recovery operation and aiding the investigation.



Bingo! Admin has recovered and restored the deleted fraudulent emails

THE END