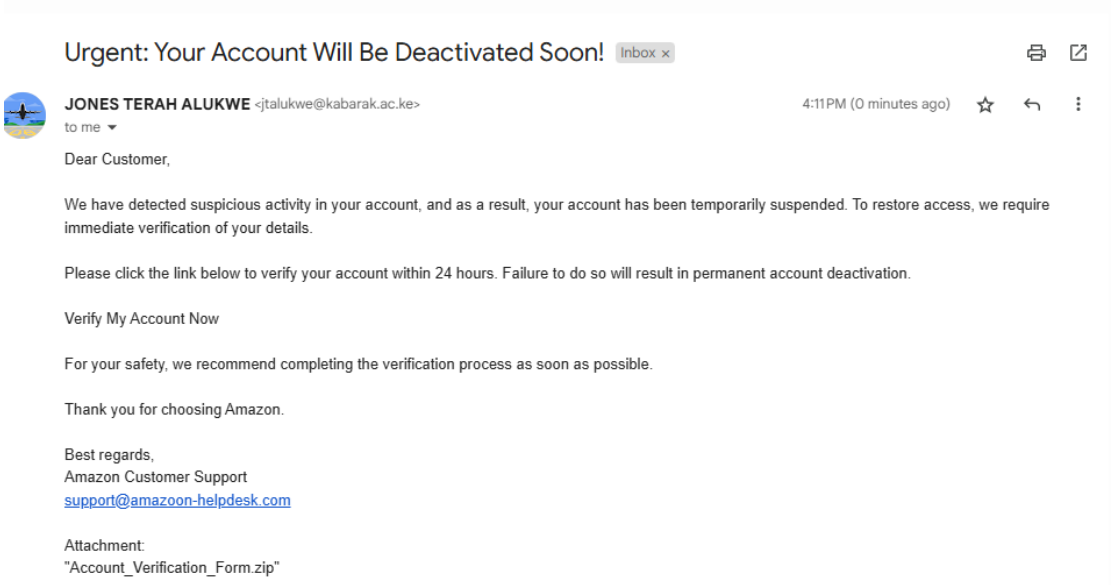
NAME: CHRISTOPHER KINYUA BAARU

EMAIL ANALYSIS REPORT

This email claims to be from Amazon Customer Support, warning the recipient of suspicious activity on their account. The message creates urgency by threatening account deactivation unless the recipient verifies their details through a provided link.



Urgent: Your Account Will Be Deactivated Soon! Inbox ×

JONES TERAH ALUKWE <jtalukwe@kabarak.ac.ke> 4:11 PM (0 minutes ago)

to me

Dear Customer,

We have detected suspicious activity in your account, and as a result, your account has been temporarily suspended. To restore access, we require immediate verification of your details.

Please click the link below to verify your account within 24 hours. Failure to do so will result in permanent account deactivation.

Verify My Account Now

For your safety, we recommend completing the verification process as soon as possible.

Thank you for choosing Amazon.

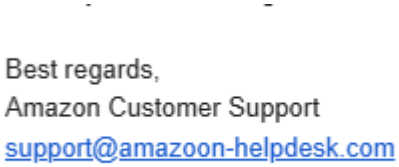
Best regards,
Amazon Customer Support
support@amazoon-helpdesk.com

Attachment:
"Account_Verification_Form.zip"

RED FLAGS IDENTIFIED

1. Suspicious Sender Email:

The sender's email address is support@amazoon-helpdesk.com, which contains a misspelling of the legitimate "amazon.com" domain. This is a clear indicator of a phishing attempt.

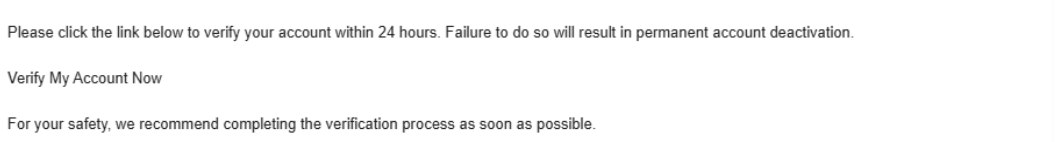


2. Urgency and Pressure:

The email employs scare tactics, warning that the recipient's account will be permanently deactivated if they do not act within 24 hours. Legitimate organizations typically avoid such pressure.

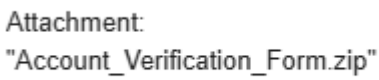
3. Fraudulent Link:

The link text says Verify My Account Now, but hovering over it reveals a suspicious URL unrelated to Amazon. This is likely a phishing site designed to steal personal information.



4. Malicious Attachment:

The email includes an attachment named "Account_Verification_Form.zip", which could contain malware. Legitimate companies rarely, if ever, send zip files for sensitive matters like account verification.



POTENTIAL IMPACT

If the recipient interacts with this email (e.g., clicking the link or opening the attachment), they could:

i. Expose their personal or financial information to attackers.
ii. Have their computer infected with malware from the attachment.
iii. Suffer identity theft, financial loss, or unauthorized account access.

RECOMMENDATIONS

1) To avoid falling victim to similar phishing attacks:
2) Verify Sender Authenticity:
3) Always double-check the sender's email address and domain. Legitimate companies use official domains (e.g., @amazon.com).
4) Avoid Clicking on Links:
5) Hover over links before clicking to verify their actual destination. If the URL looks suspicious, do not proceed.
6) Do Not Open Suspicious Attachments:
7) Avoid downloading or opening files from unknown or untrusted sources, especially compressed files like .zip.
8) Report Suspicious Emails:
9) Forward phishing emails to the company's official abuse email (e.g., stop-spoofing@amazon.com) or flag them as spam.
10) Enable Security Measures:
11) Use email spam filters, antivirus software, and two-factor authentication to enhance account security.
12) Stay Informed:
13) Regularly educate yourself about phishing tactics to identify evolving threats.