HOW TO DETECT A PHISHING EMAIL

1. DIFFERENT EMAIL ADDRESS
   - Sender's email address differs from the address of the organization they claim to be from.

2. VAGUE RECIPIENT
   - Emails may be sent to "user" or be vague because phishers do not know the recipient.

3. POOR GRAMMAR
   - Phishing emails may ask for your personal information. Organizations will NEVER ask for credentials over email.

4. URGENCY
   - Phishing emails try to tell a story or create urgency so the recipient feels a need to take action.

5. MISMATCHED OR SUSPICIOUS URLS
   - When hovering over a button or URL, the URL displayed in the link will not match the one displayed when hovering.

ID: 133 - Account Alert! (Oct. 2015)

Microsoft account team (outlooo.teeam@outlook.com)  Add to contacts 12:15 AM
To: account-security-nonreply@account.microsoft.com

Dear Outlook user,

You have some blocked incoming mails due to our maintenance problem.

In order to rectify this problem, you are required to follow the below link to verify and use your account normally.

Please click below to unlock your messages, it takes a few seconds.

Verify Your Account  http://spapparelsindia.in/Aprons/outlook.com/login.html

We apologize for any inconvenience and appreciate your understanding.

Thanks.
The Microsoft account team™