How to Identify Phishing Emails

GetApp®

How to use this deck?

The deck offers five email samples. Your task is to identify whether it is a phishing email or not.

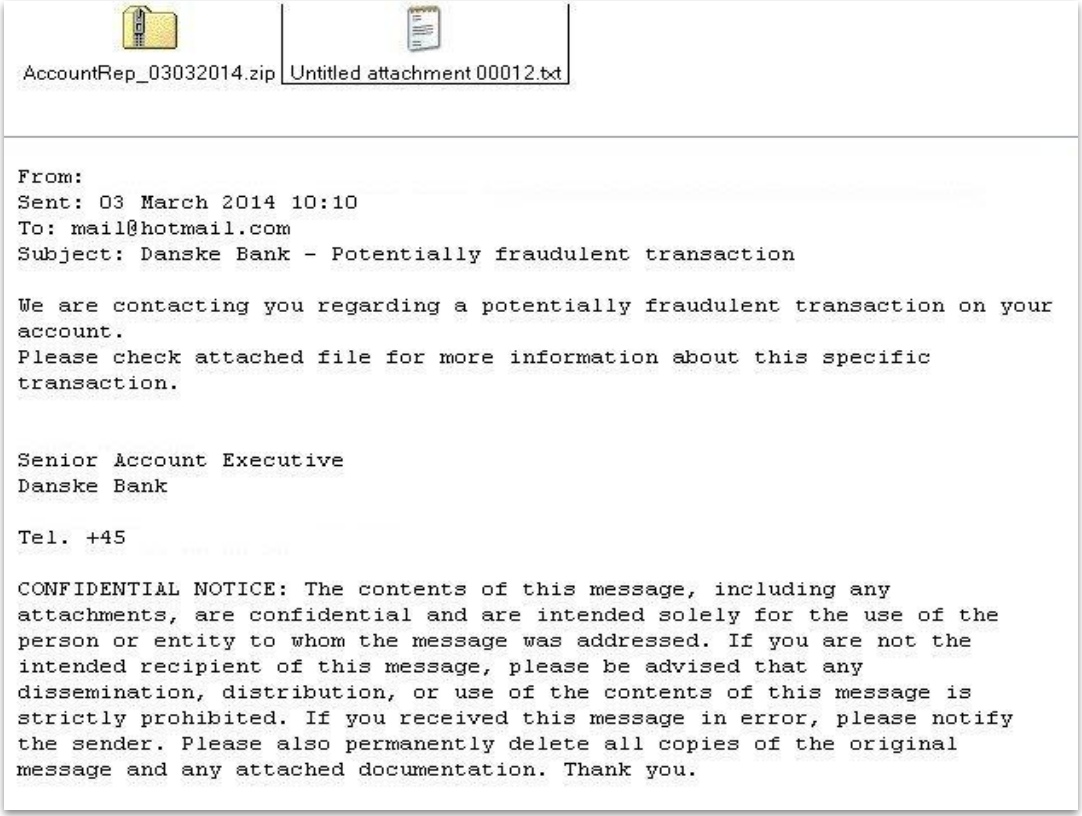
Beside each email image, we offer clues that provide evidence or support to help you identify whether the emails are fraud or not. Look at the email images first and arrive at your conclusion before you look at the clues box.

To use this deck for training purposes or to add your own training materials to it, you can:

- Download the file from the file menu (“Download as” option)
- Create a copy of the file from the file menu (“Make a copy” option)

Note: This is a view only presentation. To customize it for your business needs, you’ll need to make a copy or download it.

Email 1



Clues:

1. The sender's email address is not visible and does not have the Danske.com domain. The receipt email address looks like it was sent to many people, and not just you.

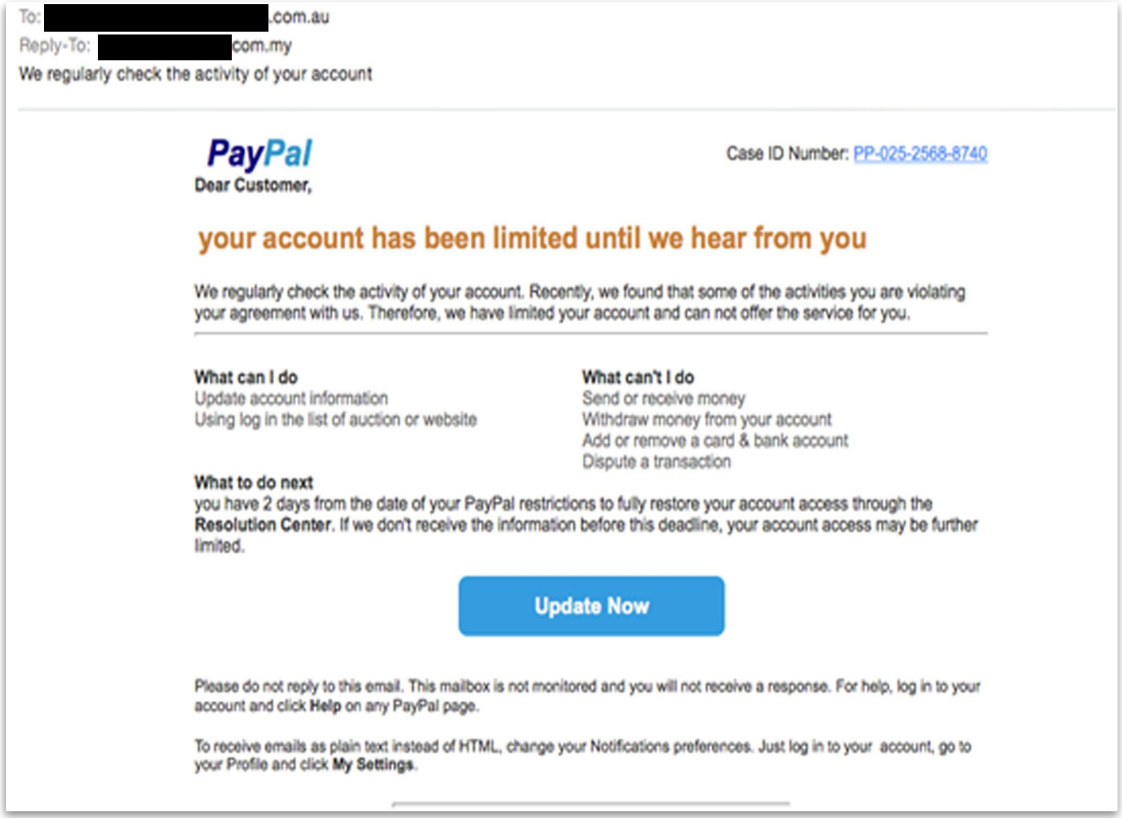
2. There is no salutation ("Dear XX")

3. Name of the sender, "Senior Account Executive," is not given, which is not typical.

4. The file names of the attachment—"Untitled"—is not typical of a professional email. Attachments are usually given specific names based on the content they hold.

Source

Email 2



To: [redacted].com.au
Reply-To: [redacted]com.my
We regularly check the activity of your account

PayPal

Case ID Number: PP-025-2568-8740

Dear Customer,

your account has been limited until we hear from you

We regularly check the activity of your account. Recently, we found that some of the activities you are violating your agreement with us. Therefore, we have limited your account and can not offer the service for you.

What can I do
Update account information
Using log in the list of auction or website

What can't I do
Send or receive money
Withdraw money from your account
Add or remove a card & bank account
Dispute a transaction

What to do next
you have 2 days from the date of your PayPal restrictions to fully restore your account access through the **Resolution Center**. If we don't receive the information before this deadline, your account access may be further limited.

Update Now

Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For help, log in to your account and click **Help** on any PayPal page.

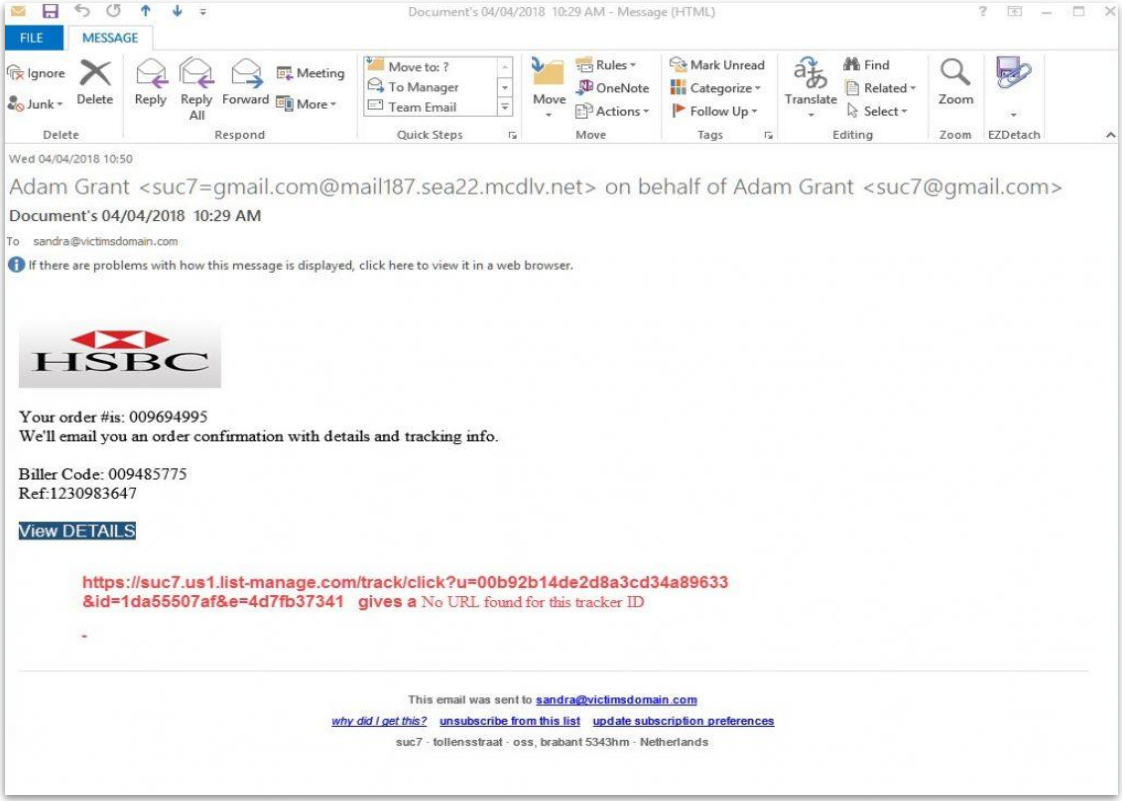
To receive emails as plain text instead of HTML, change your Notifications preferences. Just log in to your account, go to your Profile and click **My Settings**.

Clues:

1. The sender and recipient email address domain, .com.au and .com.my, are immediately suspicious.
2. There are grammatical errors in the body of the email.
3. The first words of many sentences are not capitalized.
4. The email is trying to create a sense of urgency in the reader; beware of emails that encourage you to act quickly.

Source

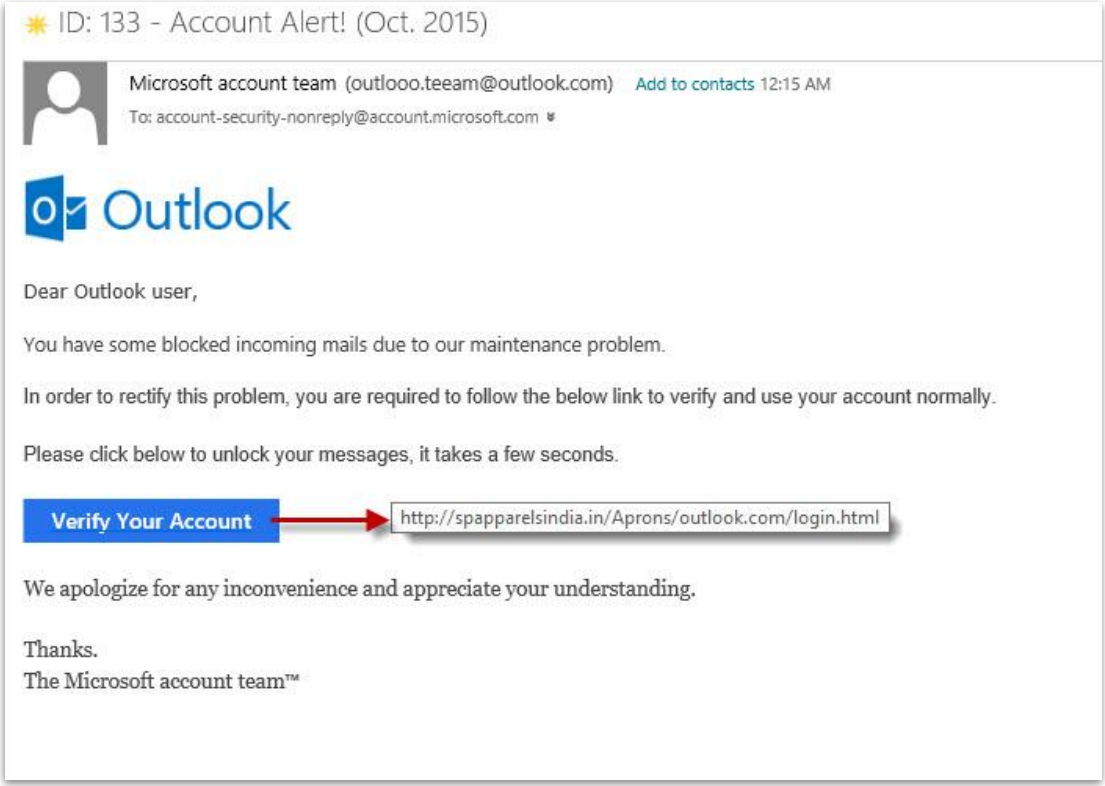
Email 3



Clues:

1. The sender's email address looks suspicious because it's not an official HSBC address.
2. The URL (in red) in the body of email again looks suspicious. Professional emails usually provide hyperlinks rather than long URLs in the body of the email.
3. There is no salutation, and the body of the email is poorly drafted.
4. Did you really make a purchase? Probably not, but the email will make you curious enough to click on the link.

Email 4



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

Outlook

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™

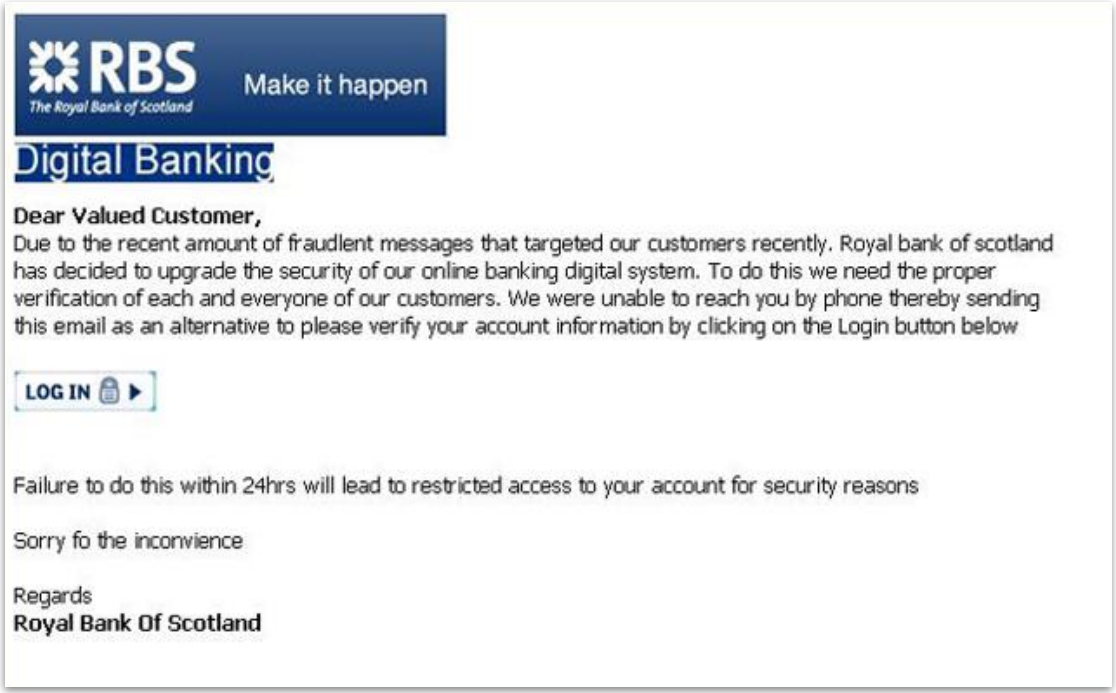
Clues:

1. Check out the sender's email address: "outloo.team@outlook.com." While it attempts to look official, the misspelling in the first word gives away the fraud.

2. Hover your mouse over URLs in the email body, and you can see it leads to a totally unrelated domain.

Source

Email 5



RBS
The Royal Bank of Scotland
Make it happen

Digital Banking

Dear Valued Customer,
Due to the recent amount of fraudlent messages that targeted our customers recently. Royal bank of scotland has decided to upgrade the security of our online banking digital system. To do this we need the proper verification of each and everyone of our customers. We were unable to reach you by phone thereby sending this email as an alternative to please verify your account information by clicking on the Login button below

LOG IN

Failure to do this within 24hrs will lead to restricted access to your account for security reasons

Sorry fo the inconvience

Regards
Royal Bank Of Scotland

Clues (this one is tricky):

1. RBS and other banks usually address their customers by name and not as “valued customer.”
2. Banks don’t ask for your PIN or to verify accounts through email.
3. It creates a sense of urgency by asking you to act within 24 hours. Beware of such tactics.
4. Check out the spelling of “inconvenience” in the last sentence. Misspellings and grammatical errors are key ways you can identify phishing emails.

Source

Key takeaways

- Double-check sender and recipient email addresses.
- Check for grammatical and spelling mistakes.
- Ensure the salutation is used correctly.
- Beware of emails that create a sense of urgency or spike your curiosity.
- Hover over URLs in the email body to check where the URL actually takes you.
- When visiting any website, check for “https:” to ensure secure web communication.

GetApp®

Your solution to every IT challenge

Rely on **GetApp.com** and **GetApp Lab** to learn more about and compare security software solutions and other technology applications.

Read about:

- **How to prevent DDoS attacks using Blockchain—and 6 more strategies**
- **Antivirus vs. Endpoint security: Which does your small business need?**
- **'Thou shalt backup thy data' : 10 Commandments for small business data backup**
- **Small business tech guide for an effective business continuity strategy**