From: mastercardslT@gmai.com

To: employee@email.com

Subject: URGENT! Password Reset Required

Body:

Hello (insert name)

Your email account has been compromised. immediate action is required to reset your password!

Click here to reset your password in the next hour or your account will be locked:

HTTPs:/en.wikipedia.org/wiki/Phishing

Regards,

Mastercard IT

From the email above, we see it's a phishing email. To identify a phishing email 3 main parts are to be considered, which are the Sender address, the grammar considering punctuation, and lastly the attachment of the email which can be a file or a link. So analyzing this email above, we can see that the sender is from a Google server (mastercardsIT@gmail.com) which indicates it's not from the company it intends to be from. The body of the email doesn't appear real or convincing so I won't spend any time on this email. Lastly, the attachment is a link that link doesn't appear real because it has nothing associating the user with any platform the sender is coming from. Analyzing the link just from the word phishing I won't click because of what it means. So my advice is to stay vigilant for what you click on the internet especially in your mail box,