How to Spot a Phishing Email

TO:

- Is the email being sent to multiple people whom you don't know?
- Was the email sent to multiple people within your office who normally would not be cc'd on the same messages?

FROM:

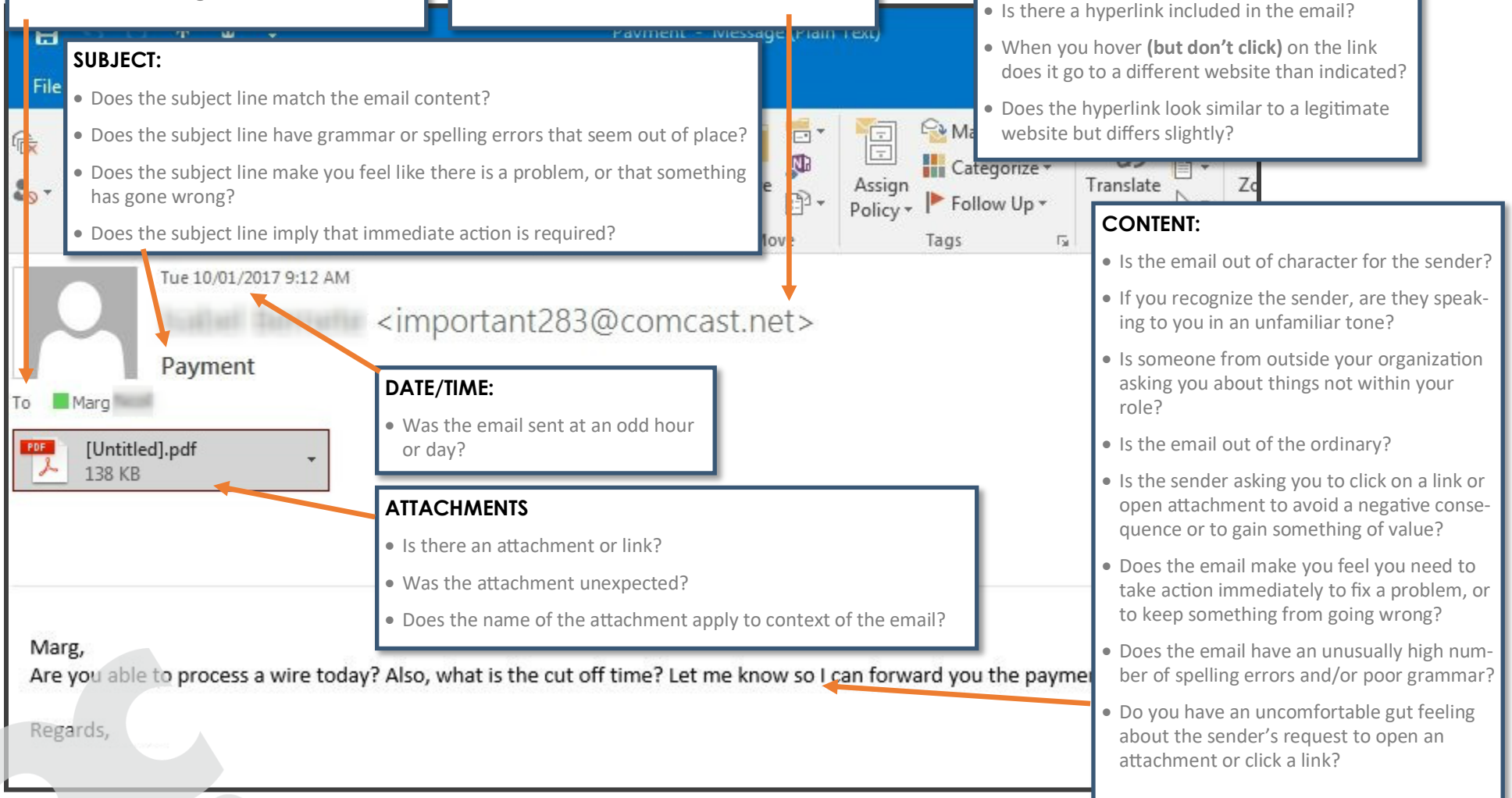
- Is the sender unfamiliar to you?
- If you recognize the name of the sender, it is different from their usual email address? *(Hover over the sender name to see their*

HYPERLINKS:

- Is there a hyperlink included in the email?
- When you hover **(but don't click)** on the link does it go to a different website than indicated?
- Does the hyperlink look similar to a legitimate website but differs slightly?

SUBJECT:

- Does the subject line match the email content?
- Does the subject line have grammar or spelling errors that seem out of place?
- Does the subject line make you feel like there is a problem, or that something has gone wrong?
- Does the subject line imply that immediate action is required?



DATE/TIME:

- Was the email sent at an odd hour or day?

ATTACHMENTS

- Is there an attachment or link?
- Was the attachment unexpected?
- Does the name of the attachment apply to context of the email?

CONTENT:

- Is the email out of character for the sender?
- If you recognize the sender, are they speaking to you in an unfamiliar tone?
- Is someone from outside your organization asking you about things not within your role?
- Is the email out of the ordinary?
- Is the sender asking you to click on a link or open attachment to avoid a negative consequence or to gain something of value?
- Does the email make you feel you need to take action immediately to fix a problem, or to keep something from going wrong?
- Does the email have an unusually high number of spelling errors and/or poor grammar?
- Do you have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?

If the answer is YES to any of the questions above, PROCEED WITH CAUTION. Think before you click.