Beware of Email Security Threats

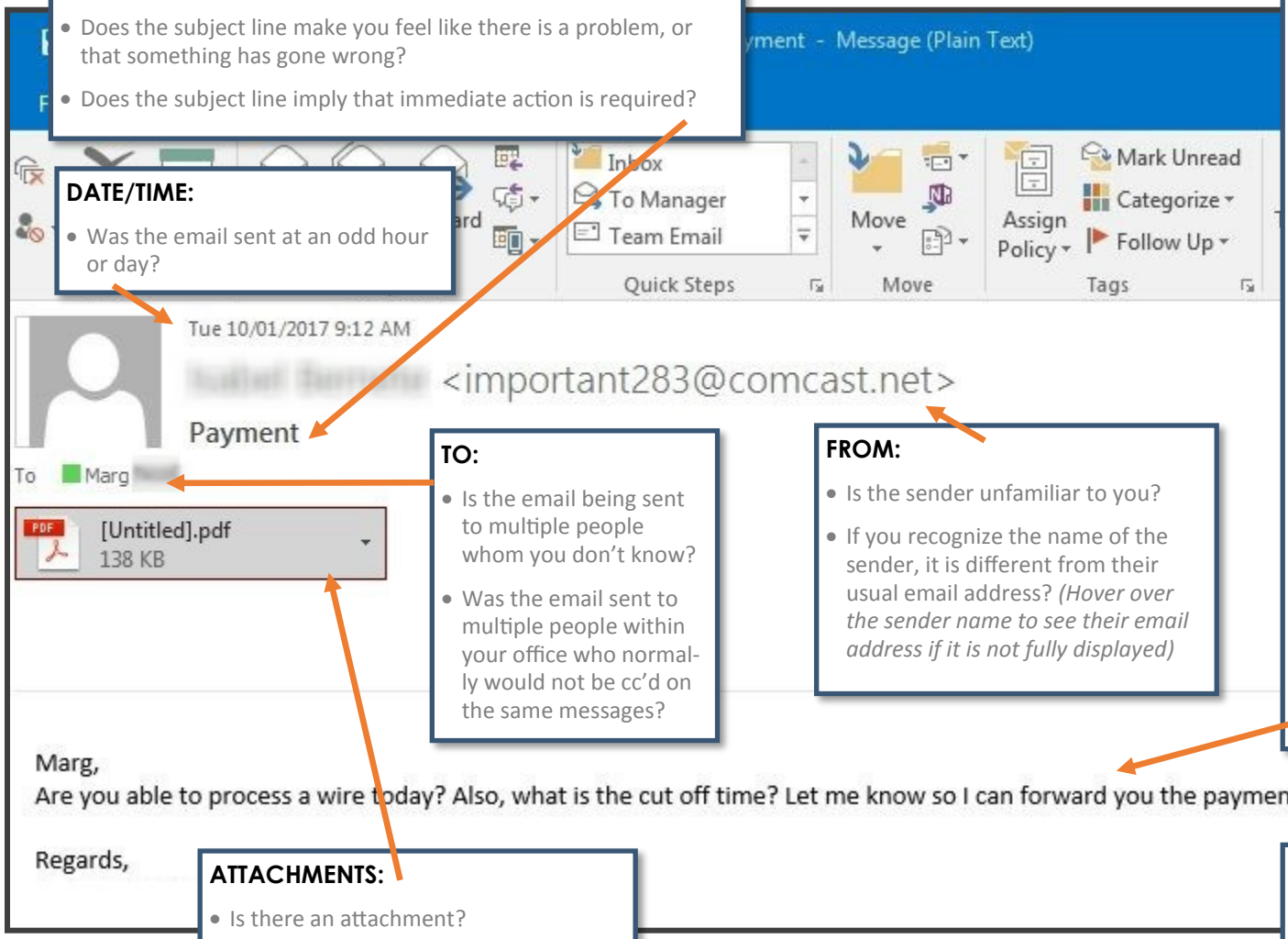
How to Recognize a Phishing Email

SUBJECT:

- Does the subject line match the email content?
- Does the subject line have language 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?



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 email address if it is not fully displayed)*

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?

ATTACHMENTS:

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

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?

If the answer is YES to any of the questions above, PROCEED WITH CAUTION.

Cyberattacks Becoming More Personal & Targeted

"Small is the new big" when it comes to cyberattacks. Smaller, more personalized malware attacks are increasing in number and sophistication with unsuspecting employees increasingly becoming the weakest link to your business' network security.

In the past, hackers have often distributed malware that took advantage of software and hardware vulnerabilities. However, as more businesses are now regularly patching their software and updating hardware, cybercriminals are putting more effort into fooling humans. Attempts to hack and attack become more personal with phishing emails containing language, references and/or requests that specifically target the receiver. Ex) An email request about payment transfers are sent to accounts payable individuals.

Educating employees on the dangers of phishing emails and their characteristics is critical to your business' network security. Taking a moment to review and verify unexpected emails before opening attachments, or providing business sensitive (or personal) information, can decrease your risk of a cyberattack. **On the next page is our guide to suspicious emails that may help you spot an email threat.**

And when in doubt, notify your I.T. department if you think you have a suspicious email or file. They can help determine if it is a threat before your business systems are infected.

PC Corp Technical Service Contact

Email: servicedesk@pccorp.com

Phone: 780 917 8281