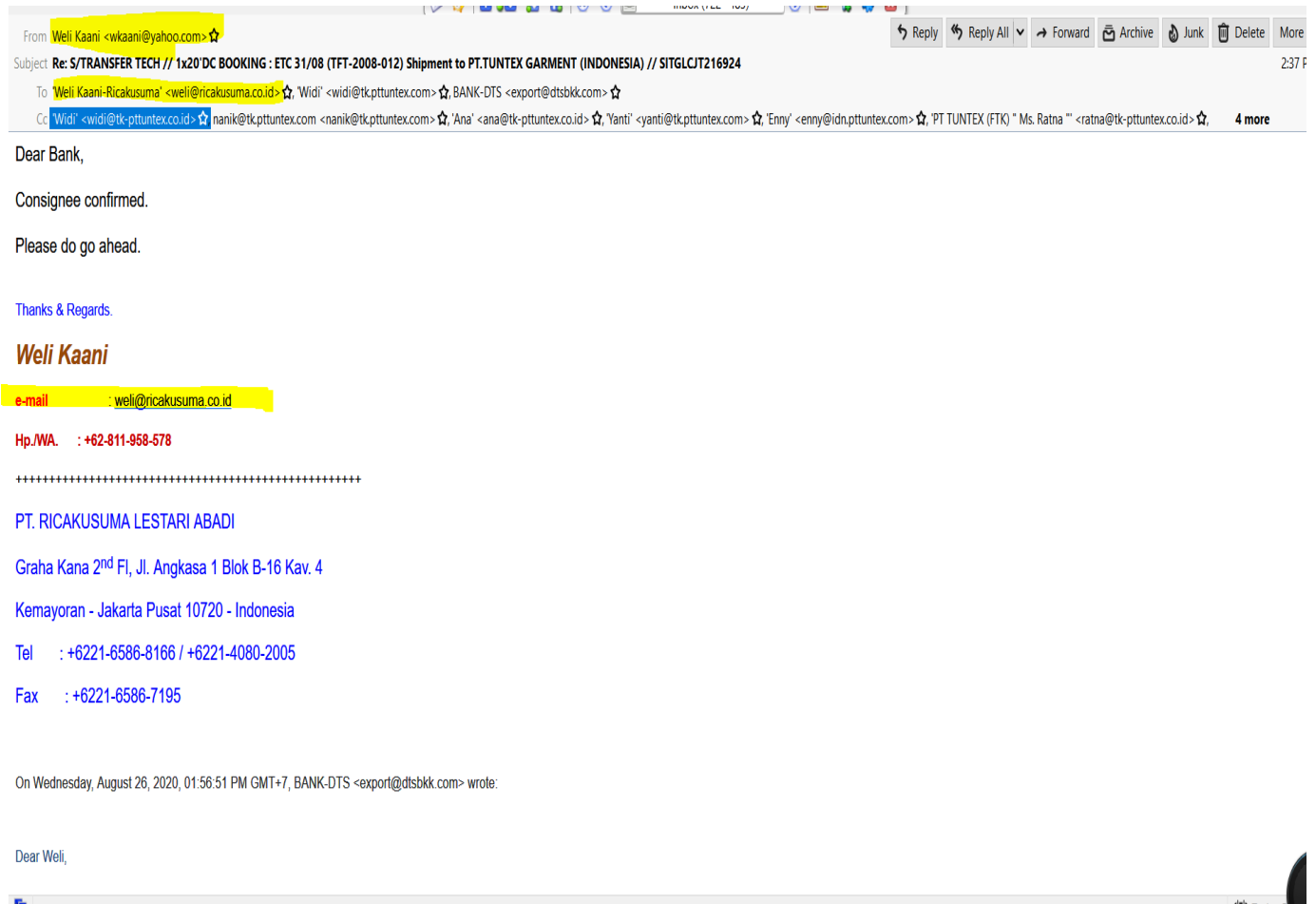# Spam Mitigating Guidelines and Best Practices

1. Always check the sender's email according to the footer or display name is it correct or not.

   - Example of spam/scam/phishing

Note: The sender email is different/incorrect

- Example of legit email which has been TAG as spam/phishing

Note: the sender email is correct.

2. As a general rule, users should not click links or download files even if they come from seemingly "trustworthy" sources.

3. Users should always be on the lookout for any grammatical errors and spelling mistakes. Legitimate companies will often employ proofreaders and editors who ensure that the materials they send out are error-free.

4. Users should not be frightened or intimidated by messages that have an alarmist tone. They should double check with the company if they are uncertain about the status of their accounts.

5. Phishing emails are designed to be sent to a large amount of people, so they need to be as impersonal as possible. Users should check whether the message contains a generic subject and greeting, as this can be a sign of a phishing attempt.

Further information on this guideline can be obtained via Tuntex IT Service Desk

https://pttuntex.com/

E-mail: itsupport@pttuntex.com