Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

June 26, 2023

Research Assignment #4

<u>Question</u>

17.3 You receive an e-mail which appears to be from your organizations personnel section, with an urgent request for you to open and complete the attached document in order to not lose a possible pay increase. But looking closely you notice that the message grammar is awkward, and that the attached file ends in .doc.zip. What should you do?

To start, you should not open or download the attachment, it is possible there are different types of malware inside this document/zipped up folder. Secondly, you should check who the email is from, although it may have someone's name you recognize you need to check the actual from address in the email to see if it is from within the organization, if it is not, report it to your security team/flag it as spam and then delete it. If it is from someone's email you recognize you should send an email to the person directly, do not press reply, to confirm with them that they sent it, if they confirm it was them then you should also call them or ask them in-person as their account may be compromised, if they say it is not them then delete it. If they confirm over the phone or in-person then you may want to ask them to send the file again and in a different format,

if they do not confirm it is them over the phone or in-person then delete the email/report it, mark as spam. Often times someone who marks an email as an urgent request, and have misspelled words or improper grammar it is because a scammer or someone who has malicious intentions are trying to make you feel in a rush as if it were truly urgent so you don't think about it and just download and open it up, you should always act carefully.

References

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Pearson.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

Dalton Murray