Discussion 2

Student’s Name

Institution

**Introduction**

Spam emails are common and usually considered as a risk to the system. It requires proper scanning before opening. However, in determination whether the email is a spam help in reducing certain risk. According to Fahad (2015), spam emails do not have a clear send of the email. The sender of email is anonymous therefore, in determination whether the email is spam the sender of email must be checked and in this case the sender was anonymous. Anonymous is regarded as unknown sender and therefore, in most cases spam emails do not have name of the sender. The spam emails is checked based on the email or domain it originates from. Spam emails keep coming from different emails with the same information. In this case, the email came from three different email addresses and therefore, it is a spam, which does not need to be considered important.

Though the email does not have obvious tail such as spelling and grammar error, there us a consistent reminder of making payment and subscribe (Washha, Khater, & Qaroush, 2012). This makes the email suspicious to a reader. However, the email is poorly written without any letter structure, and the reference is also not indicated. This makes the email vague and therefore, cannot be regarded as legitimate email. The message also lack objectivity. It only focuses on subscription and make payment to become a member, something which make readers not to trust anonymous emails. Again, there is mixture of capital and small letters throughout the message (Sarju, Thomas, & Shyni, 2014). The caps are also used more often, which makings the letter not to be regarded as official communication from an organization. Most business emails are properly written with the sender properly indicated at the end and receiver of the email is indicated as well. The email therefore, does not meet the threshold to be considered legitimate email.

# References

Fahad, S. (2015). Developing a spam Email Detector. *International Journal of Engineering and*

*Innovative Technology (IJEIT)* *, 12* (6), 2-38.

Sarju, S., Thomas, R., & Shyni, E. (2014). Spam Email Detection using Structural Features.

*International Journal of Computer Applications (0975 – 8887)* *, 8* (3), 2-35.

Washha, M., Khater, I., & Qaroush, A. (2012). Identifying Spam E-mail Based-on Statistical

Header Features and Sender Behavior. *https://www.researchgate.net/publication/316656351\_Identifying\_Spam\_E-mail\_Based-on\_Statistical\_Header\_Features\_and\_Sender\_Behavior* , 2-15.