## **Activity File: Email Security**

In this activity, you will continue to play the role of a security analyst at Acme Corp.

* Acme Corp believes that several of the suspicious emails received by the CFO are spoofed.
* You must further analyze the emails to determine which are spoofed and which are legitimate.

### **Instructions**

Open the suspicious emails provided and examine the email headers to determine which of the emails are spoofed and which are legitimate.

Answer the following questions:

* An email fails the Received-SPF verification, but was a legitimate email.  
  + What does this indicate?
  + What would you recommend to prevent future emails from failing this validation?

Always check the following:

1. Received-SPF (Pass/Fail)
2. Sender info vs email name

* Passing the SPF does not guarantee that the email is legitimate
* Failing the SPF is a strong indicator that the email is spoofed
* Matching sender info and email name does not guarantee that the email is legitimate
* Mismatching sender info and email is a likely indicator that the email is spoofed
* etc