

**Activity Overview**



In this activity, you will analyze a suspicious email and identify signs of a phishing attack. Then, you will determine whether the email should be allowed or quarantined.

Phishing is one of the most common and dangerous forms of social engineering that you’ll encounter in the field. Identifying phishing attempts will help you prevent threats and find ways to improve security procedures.

**Scenario**



Review the scenario below. Then complete the step-by-step instructions.

You’re a security analyst at an investment firm called Imaginary Bank. An executive at the firm recently received a spear phishing email that appears to come from the board of Imaginary Bank. **Spear phishing** is a malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source. In this case, the executive is being asked to install new collaboration software, ExecuTalk.

The executive suspects this email might be a phishing attempt because ExecuTalk was never mentioned during the last board meeting. They've forwarded the message to your team to verify if it’s legitimate. Your supervisor has tasked you with investigating the message and determining whether it should be quarantined.