Congratulations! You passed!

Grade received 100% **To pass** 75% or higher

Go to next item

To pass this course item, you must receive at least 75%, or 3 out of 4 points, by completing the activity and answering the corresponding questions. Once you have completed the questions, review the feedback statements. You can learn more about the graded and practice items in the course overview.

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.

Step-By-Step Instructions

Follow the instructions and answer the questions below to complete the activity.

Step 1: Analyze the suspicious email

Previously, you learned that phishing is a type of social engineering. Threat actors who send malicious emails rely on deception and manipulation techniques to trick their targets. When investigating suspicious emails like this, it's a good idea to note the threat actor's tactics. You can use that information to alert others at your organization about similar messages they might receive and what to watch out for.

Start your investigation by analyzing the suspicious message. Try to identify clues that this is a phishing attack against this executive at Imaginary Bank:

From: *imaginarybank@gmail.org*

Sent: *Saturday, December 21, 2019 15:05:05*

To: *cfo@imaginarybank.com*

Subject: *RE: You are been added to an ecsecutiv's groups*

Conglaturations! You have been added to a collaboration group 'Execs.'

Downlode ExecuTalk to your computer.

Mac® | Windows® | Android™

You're team needs you! This invitation will expire in 48 hours so act quickly.

Sincerely,

ExecuTalk©

All rights reserved.

Step 2: Examine the sender's information

1. Which two clues in the message header indicate to you that this is a phishing attempt? Select two answers. **1 / 1 point**

- [x] There is a misspelling in the subject line.

  Correct
  Two clues in the message header that indicate that this is a phishing attempt are that there is a misspelling in the subject line and the sender is using a different domain. Phishing emails commonly contain glaring spelling and grammatical errors. Another typical sign of phishing is when messages come from external domains, like a personal Gmail account.

- [x] The sender is using a different domain.

  Correct
  Two clues in the message header that indicate that this is a phishing attempt are that there is a misspelling in the subject line and the sender is using a different domain. Phishing emails commonly contain glaring spelling and grammatical errors. Another typical sign of phishing is when messages come from external domains, like a personal Gmail account.

- [ ] The subject line appears to be a reply.
- [ ] The time stamp goes beyond 12 PM.

Step 3: Review the message body for clues

Next, review the body of the message received by the executive at Imaginary Bank. Try to identify three ways this threat actor tried to disguise their message as a legitimate email.

Note: This message is strictly meant to illustrate an example of an email that contains malicious download options.

Conglaturations! You have been added to a collaboration group 'Execs.'

Downlode ExecuTalk to your computer.

Mac® | Windows® | Android™

You're team needs you! This invitation will expire in 48 hours so act quickly.

Sincerely,

ExecuTalk©

All rights reserved.

2. What details make this message appear legitimate? Select three answers. **1 / 1 point**

- [x] The download options for major operating systems

  Correct
  The brand labeling, the download options for major operating systems, and the title of the group, are all details that make this message appear legitimate.

- [x] The title of the group

  Correct
  The brand labeling, the download options for major operating systems, and the title of the group, are all details that make this message appear legitimate.

- [x] The brand labeling

  Correct
  The brand labeling, the download options for major operating systems, and the title of the group, are all details that make this message appear legitimate.

- [ ] The invitation time limit

Step 4: Investigate the download options

3. The download options open a webpage that contains a login form where someone can enter a username and password. Carefully review the webpage. What is the main clue that indicates this form is malicious? **1 / 1 point**

- (•) The URL
- ( ) Font type
- ( ) Branding
- ( ) Sign-in options

Correct
The URL is the main clue that indicates this form is malicious. Threat actors make this difficult to spot by design. When accessing SaaS services, like Microsoft applications, the URL typically includes the organization's domain.

4. After completing your investigation, should this email be quarantined? **1 / 1 point**

- (•) Yes
- ( ) No

Correct
Thank you for completing this activity! Phishing emails come in many forms and can be difficult to spot when they are well disguised. Security analysts routinely handle email analysis and remediation. Identifying malicious emails can be much easier when you know which clues to look for. Review the quiz feedback to find out how you did.