**Suspicious email through phishing  
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 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.

1. Which two clues in the message header indicate to you that this is a phishing attempt? Select two answers.
2. There is a misspelling in the subject line.
3. The time stamp goes beyond 12 PM.
4. The subject line appears to be a reply.
5. The sender is using a different domain.
6. What details make this message appear legitimate? Select three answers.
7. The download options for major operating systems
8. The invitation time limit
9. The brand labeling
10. The title of the group
11. 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?
12. The URL
13. Branding
14. Font type
15. Sign-in options
16. After completing your investigation, should this email be quarantined?

Yes

No

## Answers

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

A. There is a misspelling in the subject line.

D. The sender is using a different domain.

The email is coming from "[imaginarybank@gmail.org](mailto:imaginarybank@gmail.org" \t "_new)," which is a different domain than the official domain for Imaginary Bank. Legitimate communications from Imaginary Bank would likely come from their official domain.

1. What details make this message appear legitimate? Select three answers.

A. The download options for major operating systems

The inclusion of download options for different operating systems makes the phishing attempt more sophisticated, but it doesn't necessarily make the message legitimate.

B. The invitation time limit

The urgency created by the 48-hour time limit is a common phishing tactic to prompt quick action, but it doesn't make the message legitimate.

C. The brand labeling

The inclusion of the ExecuTalk© brand is an attempt to add legitimacy to the message, but it's not a guarantee of authenticity.

1. 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?

A. The URL

The URL is a crucial indicator. Legitimate organizations typically use secure and recognizable domains. In this case, the use of a Gmail domain ("[imaginarybank@gmail.org](mailto:imaginarybank@gmail.org" \t "_new)") in the email and potentially in the URL is a strong indication of a phishing attempt.

1. After completing your investigation, should this email be quarantined?

A. Yes

Given the indications of phishing, such as the use of a different domain and the potential malicious URL, it would be advisable to quarantine this email to prevent the executive from falling victim to a phishing attack.

it's always essential to educate users about phishing techniques and encourage them to verify the legitimacy of unexpected or suspicious emails before taking any action.

Top of Form

Bottom of Form