Step-By-Step Instructions

Follow the instructions and fill in the sections 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

Next, examine the major parts of this message in closer detail starting with the email header. You can often find clues in the message header that indicate you are dealing with a phishing attack.

Examine the email header of this suspicious message:

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*

—---

Pro tip: Always check the domain name that comes after the @ symbol. Requests for sensitive information or asking you to download files should not come from personal accounts, like *@gmail.com, @icloud, @yahoo.com* or others.

Questions

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

    a. The sender is using a different domain.
    b. The subject line appears to be a reply
    c. The time stamp goes beyond 12 p.m.
    d. There is a misspelling in the subject line.

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**.**

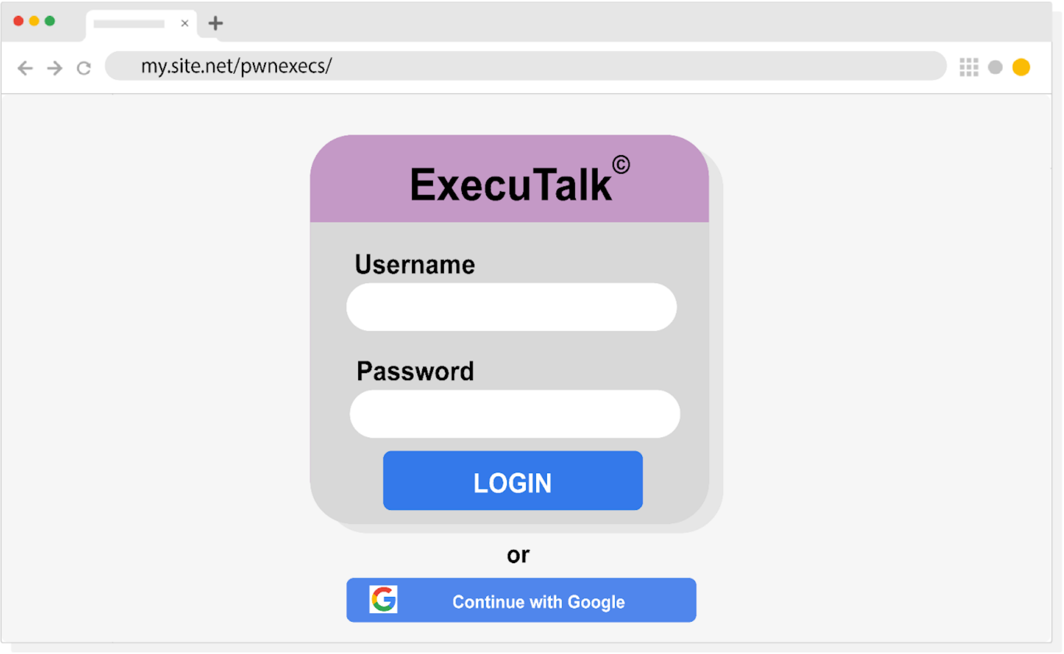
    a. The brand labeling
    b. The download options for operating systems
    c. The invitation time limit
    d. The title of the group

Step 4: Investigate the download options

Phishing emails often contain links that redirect to malicious sites or trigger malware downloads.

Pro tip: When investigating suspicious emails, hovering your mouse cursor over buttons will reveal the URL they redirect to without having to click them. This is the safest way to check if it will take you to a suspicious domain or if it links to an http:// URL that isn't secure.

In this case, the message contains three download options. Each of them opens this login form:



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

a. Font type
b. Sign-in options
c. Branding
d. The URL

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

a. Yes
b. No