Self-reflection: Filter malicious emails-My-Responses.docx

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.

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.

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

The sender is using a different domain.

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©

2.

Question 2

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

The title of the group

The download options for major operating systems

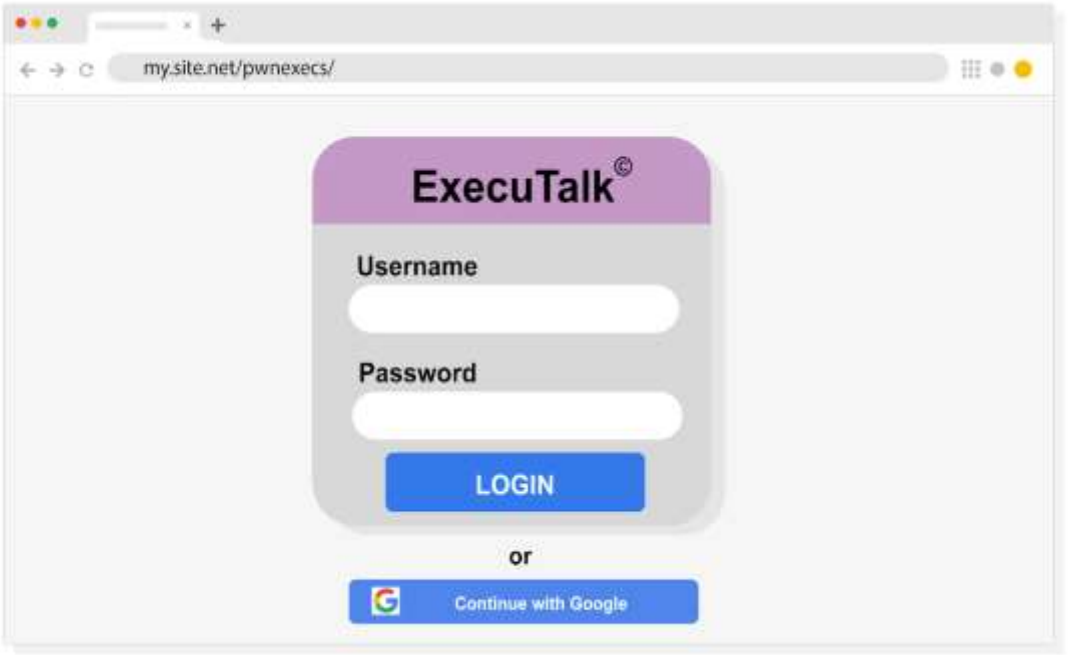
The brand labeling

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:



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?

The URL

Question 4

After completing your investigation, should this email be quarantined?

Yes

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.