# **Activity: Filter malicious emails**

**Scenario**



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. 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. Analyse the suspicious email**

**A screenshot of a email

Description automatically generated**

**Step 2. Examine the sender’s information**

**A screenshot of a computer

Description automatically generated**

**The sender is using a .org domain, and there is a misspelling in the subject line. This indicates that this is a phishing attempt.**

**Step 3. Review the message body for clues**

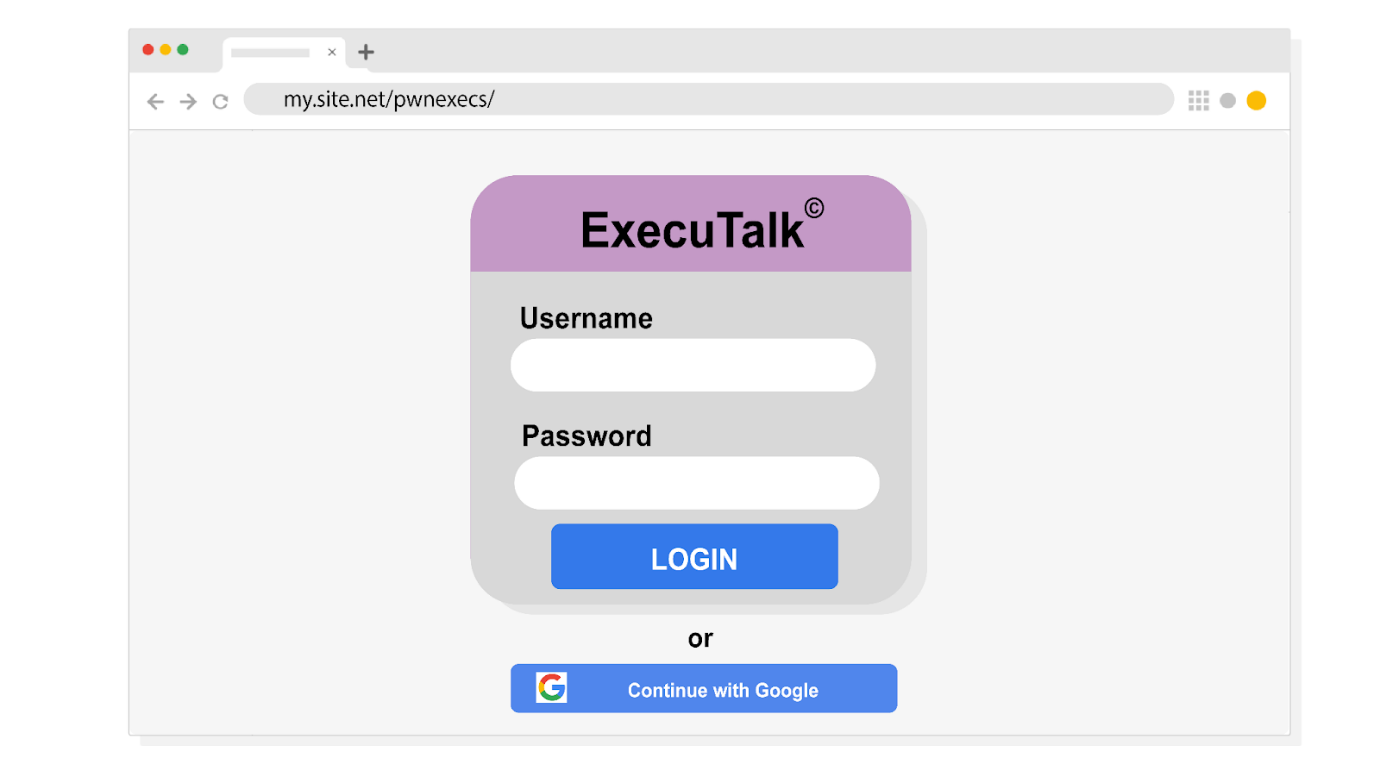
**A screenshot of a white card

Description automatically generated**

**The brand labelling, the download options for major operating systems and the title of the group make this email appear legitimate.**

**Step 4. Investigate the download options**

**The message contains three download options. Each of them opens this login form:**

****

**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.**

**The main clue that indicates this form is malicious is the URL.**

**After completing the investigation, this email should be quarantined.**